Enabling Secure Online Elections with the Voting Service Provider

Vom Fachbereich Informatik
der Technischen Universität Darmstadt
genehmigte

Dissertation

zur Erlangung des Grades
Doctor rerum naturalium (Dr. rer. nat.)
von

Dipl.-Math. Axel Tobias Schmidt
geboren in Darmstadt

Referenten:	Prof. Dr. Johannes Buchmann
	Prof. Dr. Peter Ryan
Tag der Einreichung:	25. August 2012
Tag der mündlichen Prüfung:	29. Oktober 2012

Darmstadt 2012
Hochschulkennziffer D 17

Erklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit – abgesehen von den in ihr ausdrücklich genannten Hilfen – selbständig verfasst habe.

Axel Tobias Schmidt

Wissenschaftlicher Werdegang

Mai 2006 – April 2010

Wissenschaftlicher Mitarbeiter und Promotionsstudent bei Prof. Johannes Buchmann am Lehrstuhl Kryptographie und Computeralgebra im Fachbereich Informatik der Technischen Universität Darmstadt

Oktober 1999 – April 2006

Studium der Mathematik mit Schwerpunkt Informatik an der Technischen Universität Darmstadt

Acknowledgments

I would like to thank Johannes Buchmann, Peter Ryan, Melanie Volkamer, Dennis Heinson, Philipp Richter, Lucie Langer, Alex Wiesmaier, Richard Lindner, Anja Lehmann, Marita Skrobic, and Roswitha Jäger-Beck.

Axel Schmidt
Frankfurt am Main, 2012

Abstract

Online voting promises to improve the experience of democratic participation. For example, it allows convenient vote casting from home or office and speeds up the tallying process. While this may increase voter turnout on the one hand, it is supposed to reduce costs and efforts on the other hand.

The security of online elections is of crucial importance. Many security requirements have to be satisfied in order to achieve at least the basic election principles of a universal, free, equal, and secret election. Today's online voting protocols claim to achieve these security goals. However, in order to securely implement and operate such protocols, a secure operational environment is necessary. It must satisfy many technical and organizational requirements like for example providing the secure IT infrastructure including secure hardware and software, secure server rooms and secure communication channels, as well as qualified election organization, expert knowledge and skilled personnel. Preparing an operational environment accordingly is complex and costly. While this makes online voting impractical and reduces its potential benefits, an insufficient or faulty operational environment would even endanger the security of online elections.

One approach to solve these problems is the concept of a Voting Service Provider (VSP). The idea is to outsource the technical implementation of an online election to a professional and qualified service provider. The VSP technically carries out the election on behalf of the Election Host, i.e. the party which intends to hold the election. To this end, the VSP provides the secure operational environment, the secure online voting software, and the expert knowledge and securely implements the online election. This reduces efforts and costs for the Election Host and enables secure online elections.

In this thesis we analyze the VSP concept and develop an approach to verifiably ensure the security of online elections with VSPs. Our approach is based on a legal regulation for VSPs that defines the requirements for secure online elections in compliance with applicable law. We derive corresponding technical requirements for the online voting software and the operational environment of VSPs and include them in a Security Concept Template. The template is used as the basis to verify the security of VSPs. To this end, we develop an overall approach for the evaluation and certification of VSPs based on the Common Criteria and IT-Grundschutz methodologies. We finally provide implementation proposals for the VSP and its secure operational environment and thereby demonstrate the feasibility of the concept.

Our work provides a deeper understanding of the operational environment of online elections and its significance for the security. We introduce the VSP as a new concept to realize secure online elections. We thereby demonstrate that the technique of outsourcing can be applied to the field of online voting. We identify the technical requirements for both the online voting software and the operational environment as a foundation for secure online elections. Our results are of general value to assess the overall security of online voting systems. The introduced evaluation and certification concept addresses the online voting software and the operational environment altogether for the first time and makes the overall security of online elections verifiable. The implementation proposals help realizing the necessary secure operational environment. Our security approach is

embedded in a legal regulation and thereby lays the foundation for legally binding online elections.

Zusammenfassung

Onlinewahlen versprechen, das Erlebnis der demokratischen Partizipation zu verbessern. Sie ermöglichen zum Beispiel die bequeme Stimmabgabe von zuhause oder vom Arbeitsplatz und beschleunigen den Auszählungsprozess. Dies kann einerseits die Wahlbeteiligung erhöhen und soll andererseits Aufwand und Kosten reduzieren.

Die Sicherheit von Onlinewahlen ist von entscheidender Bedeutung. Zahlreiche Sicherheitsanforderungen müssen erfüllt werden, um zumindest die grundlegenden Wahlprinzipien der allgemeinen, freien, gleichen und geheimen Wahl zu gewährleisten. Heutige Onlinewahlprotokolle geben an, diese Sicherheitsziele erreichen zu können. Um derartige Protokolle jedoch sicher zu implementieren und zu betreiben, ist eine sichere Einsatzumgebung notwendig. Sie muss viele technische und organisatorische Anforderungen erfüllen, zum Beispiel die sichere IT Infrastruktur inklusive sicherer Hardware und Software, sicherer Serverräume und Kommunikationsverbindungen sowie die qualifizierte Organisation der Wahl, Fachkenntnisse und geschultes Personal bereitstellen. Eine Einsatzumgebung entsprechend zu präparieren ist aufwendig und kostspielig. Während Onlinewahlen dadurch unpraktisch werden und ihr potenzieller Nutzen reduziert wird, würde eine unzureichende oder fehlerhafte Einsatzumgebung sogar die Sicherheit von Onlinewahlen gefährden.

Ein Ansatz, diese Probleme zu lösen, ist das Konzept des Wahldiensteanbieters (WDA). Die Idee ist, die technische Durchführung eine Onlinewahl an einen professionellen und qualifizierten Diensteanbieter auszulagern. Der WDA führt die Wahl im Auftrag des Wahlausrichters durch, also desjenigen, der beabsichtigt, die Wahl auszurichten. Zu diesem Zweck stellt der WDA die sichere Einsatzumgebung, die sichere Wahlsoftware und die Fachkenntnis bereit und führt die Onlinewahl sicher durch. Dies reduziert Aufwand und Kosten für den Wahlausrichter und ermöglicht sichere Onlinewahlen.

In dieser Dissertation untersuchen wir das WDA Konzept und entwickeln einen Ansatz, um die Sicherheit von Onlinewahlen nachweislich sicherzustellen. Unser Ansatz basiert auf einer gesetzlichen Regelung für WDAs, die die Anforderungen für sichere Onlinewahlen in Übereinstimmung mit geltendem Recht definiert. Wir leiten daraus technische Anforderungen für die Onlinewahlsoftware und die Einsatzumgebung von WDAs ab und erstellen daraus eine Sicherheitskonzeptvorlage. Diese Vorlage bildet die Grundlage für die Überprüfung der Sicherheit von WDAs. Zu diesem Zweck entwickeln wir einen ganzheitlichen Ansatz für die Evaluierung und Zertifizierung von WDAs, der auf den Common Criteria und IT-Grundschutz Methoden aufbaut. Schließlich machen wir Umsetzungsvorschläge für den WDA und seine sichere Einsatzumgebung und weisen damit die Machbarkeit des Konzepts nach.

Unsere Arbeit liefert ein tieferes Verständnis der Einsatzumgebung von Onlinewahlen und ihrer Bedeutung für die Sicherheit. Wir stellen den WDA als neues Konzept zur Realisierung von sicheren Onlinewahlen vor. Dadurch zeigen wir, dass die Technik des Outsourcing im Bereich der Onlinewahlen angewendet werden kann. Als eine Grundlage für sichere Onlinewahlen identifizieren wir die technischen Anforderungen für sowohl die Onlinewahlsoftware als auch die Einsatzumgebung. Unsere Ergebnisse sind von allgemeinem Wert, um die ganzheitliche Sicherheit von Onlinewahlsystemen bewerten zu

können. Das vorgestellte Evaluierungs- und Zertifizierungskonzept adressiert erstmals die Onlinewahlsoftware und die Einsatzumgebung gemeinsam und macht die ganzheitliche Sicherheit von Onlinewahlen nachweisbar. Die Umsetzungsvorschläge helfen dabei, die notwendige sichere Einsatzumgebung zu realisieren. Unser Sicherheitsansatz ist in eine rechtliche Regelung eingebettet und schafft so die Voraussetzung für gesetzlich verbindliche Onlinewahlen.

Contents

1. Introduction

Voting is the central instrument for democratic participation. The new technology of online voting promises to modernize and improve the electoral practice. It allows voters to conveniently cast their vote from home or office using their computer or mobile device. This may increase voter turnout. The voters are enabled to verify the election process and its outcome. This may improve the trustworthiness of the election procedure. Furthermore the information technology promises to simplify the implementation of the election. For example the election result can be determined within seconds. This is supposed to reduce efforts and costs which is in particular attractive for non-political elections like the election of a works council in a company. Such companies intend to save money by implementing online voting systems. Online elections have been successfully implemented several times. In 2007, Estonia was the first country to implement online voting in parliamentary elections [108, 55]. Another example is the election of the chairmanship of the German Informatics Society which has been carried out electronically since 2004 using the Polyas online voting system [70, 88]. In 2009, the Austrian students elected the representative body of the Austrian Students Union via Internet [31]. Moreover, in March 2009, the presidential election at the Université catholique de Louvain in Belgium were held using the Helios online voting system [28]. However, several challenges have to be faced when implementing online elections.

1.1. Motivation of the Voting Service Provider

Online elections must be secure. Secure means to observe the security goals that derive from the applicable election principles of at least a universal, free, equal, and secret election. In the field of electronic voting, among the most important security goals are *accuracy* (votes cannot be altered, duplicated or eliminated, all valid votes are counted correctly, and invalid votes are not counted), *democracy* (only eligible voters are permitted to cast their vote and only one vote per voter is accounted), *anonymity* (it must be impossible to associate a vote with the voter who cast it), *receipt-freeness* (a voter must not be able to prove in which way he voted), *uncoercibility* (a voter cannot be forced to abstain from voting or to vote in a particular way), and *verifiability* (all voters can verify that the votes were counted correctly) [93, 78, 86]. Online voting protocols have been studied thoroughly. Several systems have been introduced that claim to achieve these security goals, for example the protocols of Juels et al. [79], Adida [27], Lee and Kim [86], Baudron et al. [34], or Ohkubo et al. [91].

However, in order to securely implement and operate such online voting protocols, a secure operational environment is necessary. Hence, when an election operator wants

to implement a secure online election he must provide a secure operational environment and operate a secure online voting system therein. To this end, the election operator must satisfy many security requirements and implement corresponding safeguards. For example, it must provide at least the secure IT infrastructure including secure hardware and software to run the voting system, a secure building where the election servers are safely operated, a secure communication network to provide secure access for the voters, the secure management of cryptographic keys and authentication means, as well as qualified organization of the election and the specialist knowledge and skilled personnel necessary to securely operate the voting system. Preparing the operational environment to satisfy these requirements is a complex and costly task that involves considerable effort and requires comprehensive skills on the part of the election operator. This renders online voting impractical for most election operators and reduces its potential benefits. More important, an insufficient or faulty operational environment would endanger the security of the online election. So far there is no concept that verifiably ensures the security of the operational environment for online elections.

The concept of a Voting Service Provider (VSP) is able to solve these problems. The VSP is a qualified and professional service provider that technically implements an online election on behalf of the Election Host, i.e. the party which wants to hold the election. To this end, the VSP provides both the secure operational environment and the secure online voting software and possesses the necessary expert knowledge to securely implement the online election. While realizing the secure operational environment is costly and impractical for the Election Host that needs to perform elections only rarely, it does make sense for a VSP that implements secure online elections as a business and hence more frequently. In fact, the VSP concept might even represent a business model which would possibly stimulate business interest in realizing secure online elections. The VSP unites the secure voting software and the secure operational environment. This enables an approach based on legal regulation, overall evaluation and certification, and accreditation to ensure and verify the security of online elections. This approach has proven successful for example in the similar case of Certification Authorities (CAs) which issue and manage cryptographic keys and certificates in a Public Key Infrastructure (PKI).

Another approach to strengthen security in electronic elections is to use cryptographic voting protocols that achieve as many security requirements as possible. For example, various "end-to-end verifiable" protocols have been proposed that provide guarantees of the integrity of the election process and its outcome without the need to trust the voting system or the election operator (see [81] for a definition). Regarding supervised schemes, the *Prêt à Voter* voting protocol introduced by Ryan [94, 45], for example, enables the voter and the public to check the correctness of the election process and the outcome based on receipts and a bulletin board. The *Scantegrity* scheme introduces confirmation codes that allow voters to verify that their votes are included correctly while the public is enabled to check that the election result is computed accurately [44]. But this property can also be found in online voting schemes such as *Pretty Good Privacy*. This protocol uses a threshold set of trustees to provide the verifiability properties "Cast as Intended" and "Counted as Cast and Tallied Correctly" [95]. While using different techniques all these protocols aim to provide end-to-end verifiability with minimal dependence on for

example correct code or trustworthy operation of the voting system. In such cases, the operational environment would be relieved of addressing those requirements by means of additional organizational or technical measures. However, even with such verifiable protocols there remain many security requirements that cannot be fulfilled by the voting protocol alone. The technical capabilities to enforce security properties in software are limited. For example, Schneider showed that certain property classes cannot be enforced using execution monitoring techniques [97]. For properties like confidentiality or availability we need organizational, procedural support by the operational environment. Even for integrity, procedural support by the operational environment is typically needed: maintaining an accurate electoral roll, authentication mechanisms to enforce eligibility, ensuring only one vote per voter is counted or countering ballot-stuffing. To sum up, a secure operational environment is always necessary, and the VSP concept will always increase the assurance of election security. The goal of this thesis is therefore to demonstrate that the VSP enables secure online elections. To this end, we will explore the VSP concept and elaborate the aforesaid security approach.

1.2. Research Question, Contributions and Thesis Outline

This thesis aims at answering the following research question:

How to enable secure online elections with a VSP?

To answer this question, we approach the issue in several steps following the KORA methodology (KOnkretisierung rechtlicher Anforderungen, engl. Concretizing legal requirements, see [72]). KORA is an approved methodology to bridge the gap between law and technology. To this end, a four step procedure translates abstract legal requirements to the technical field in order to make them technically utilizable. In the first step, legal requirements are identified based on constitutional law and other applicable statutes. In step two, these abstract requirements are further specified to establish a closer relation with the technical context. Then technical requirements are derived by incorporating state-of-the-art technical documentation which is used to technically refine the previous results. At last, a design proposal demonstrates a technical implementation. Summarizing, KORA allows to design technical systems in compliance with the law. We extend the KORA methodology in order to make the legal compliance and thus the security of VSPs verifiable. Therefore we develop an evaluation and certification approach based on Common Criteria [42] and IT-Grundschutz (engl. IT Baseline Protection, [62]) that allows to verify that a VSP satisfies all security requirements in compliance with the law.

We implement this approach in the following way. At first, we present a *legal regulation* that defines the requirements for secure online elections with VSPs according to applicable law[1]. The regulation consists of an act and an ordinance. We identify the

[1]The legal regulation has been developed by jurists in cooperation with a team of IT experts in which the author of this thesis participated.

contained legal requirements and more specific legal criteria according to the first and the second KORA step. Then we derive technical requirements for VSPs and include them in a *Security Concept Template*. To this end, we implement the third KORA step and concretize the legal criteria using current technical documentation into technical requirements for both the online voting software and the operational environment of VSPs. The Security Concept Template contains all requirements of the legal regulation in a technical interpretable form and thus serves as the foundation for the legally compliant design as well as the security evaluation and certification of VSPs. Next, we introduce an *evaluation, certification and accreditation* approach. The evaluation and certification procedure allows to verify that a VSP indeed satisfies all technical requirements of the Security Concept Template and thus is compliant to the legal regulation. Based on the result, an official authority accredits the VSP and thereby confirms its security capability and legal compliance. To prove the feasibility of this approach, we demonstrate that the Common Criteria and the IT-Grundschutz methodologies can be applied to evaluate and certify the VSP's online voting software and its operational environment respectively. To this end, we show how the Common Criteria Protection Profile (PP) for online voting products [64] and the IT-Grundschutz safeguards [59] can be used to satisfy the previously identified technical requirements. At last, we use these results to provide a *design proposal* of a VSP. For this purpose, we provide a detailed specification based on the realistic scenario of the Austrian Students Union election in 2009 [31] and the online voting protocol from Scytl [99]. We thereby demonstrate the functionality and the feasibility of the VSP concept in practice. We identify suitable IT-Grundschutz safeguards to show that the VSP is able to implement the required secure operational environment for online elections.

Now we sum up the contributions of this thesis. Our work brings the operational environment of online elections into the research focus and provides a deeper understanding of its significance for the security. We present the VSP as a new concept to approach the overall security of online elections. The VSP introduces the idea of outsourcing to the field of electronic voting. We demonstrate that the VSP makes secure outsourcing of online elections possible and thereby enables their secure implementation in a practical way. This alternative approach brings a new perspective to the research field. By embedding the VSP concept in a legal regulation we lay the foundation to enable legally binding online elections for the first time in Germany[2]. This facilitates the entrance of the online voting technology into practice and allows introducing online voting as an alternative voting channel in legally regulated election scenarios. For our security approach, we identify the technical and organizational requirements that the voting software and the operational environment must satisfy in order to enable secure online elections in compliance with the law. The resulting template facilitates the evaluation and certification of VSPs, but is of general value to assess the security of all online voting systems. Moreover, the template ensures a consistent and comparable security

[2]In Germany, legal regulation in the field of electronic voting currently restricts to regulating the use of electronic voting machines for polling stations (see the German Federal Electoral Act [7] and the German Federal Voting Machines Ordinance [18]).

level among accredited VSPs. In the similar scenario of CAs in Germany, such template does not exist. We provide an evaluation and certification approach that addresses both the online voting software and the operational environment for the first time. Thereby we enhance the current standard of pure software evaluation and certification based on the Common Criteria PP for online voting products [64]. Furthermore, we provide a design proposal that helps implementing the secure operational environment to realize legally compliant online elections. To sum up, we present a practical concept that enables verifiably secure and legally compliant online elections.

The thesis is organized as follows. In Chapter 2 we introduce the VSP concept. Therefore we describe the basic setup and the processes and consider the election procedure with a VSP. We present our approach to enable the security of VSPs and describe the KORA methodology in Chapter 3. The legal regulation for VSPs can be found in Chapter 4. We derive the technical requirements for VSPs and present the Security Concept Template in Chapter 5. The evaluation, certification and accreditation approach is presented in Chapter 6. The VSP design proposal can be found in Chapter 7. In Chapter 8 we review the VSP concept and discuss related issues. We conclude the thesis in Chapter 9 by summarizing the results and considering open questions and future work.

2. The Voting Service Provider Concept

The goal of this chapter is to define the Voting Service Provider (VSP). To this end we derive the objective of the VSP and present the actors, the architecture and the processes. Then we describe the particular properties of the VSP concept. This chapter is based on work we published in [P9] and [P10].

2.1. Objective and Actors

In this section we derive the objective of the VSP. Therefore we identify the VSP's function within the scenario of an online election. While doing so we introduce the involved actors. We illustrate an overview in Figure 2.1.

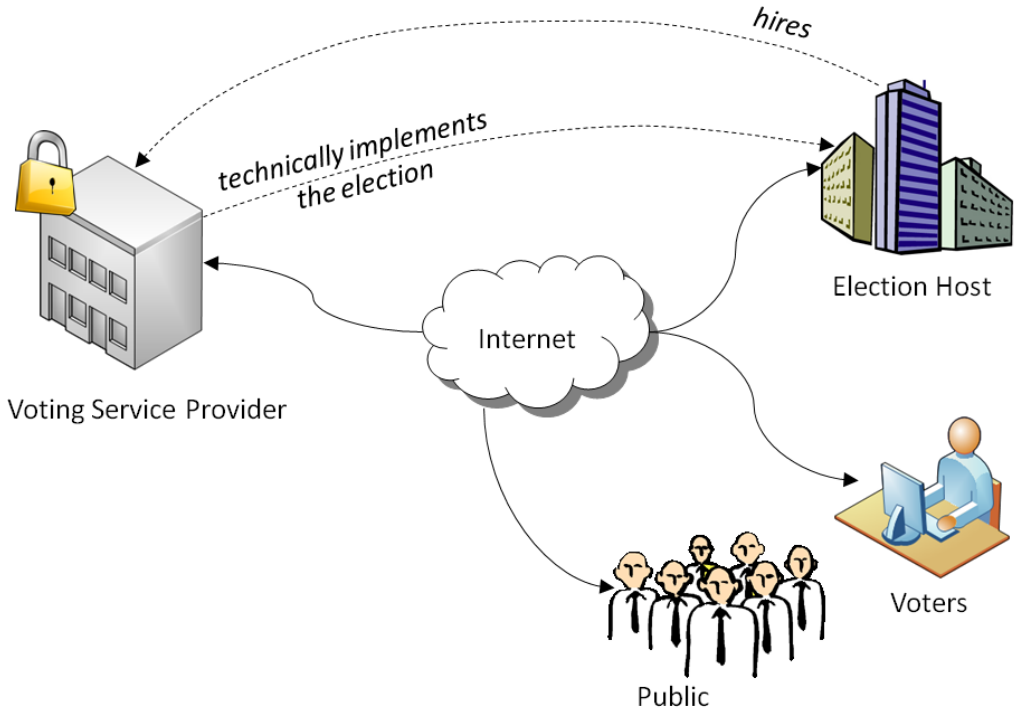

Figure 2.1.: The VSP concept

In a classic election scenario there are the *Voters*, the *Public*, and the *Election Host.* Now we expand this set up by the *VSP.* The Election Host is responsible for organizing the election. He has the primary interest in the election and its outcome. The law dictates rules to the Election Host that prescribe the obligations he has to fulfill. In order to discharge those duties the Election Host requires the technical equipment and expertise necessary for performing a secure online election. The Election Host can delegate that to a VSP. Thus the VSP takes on the technical implementation of the online election on behalf of the Election Host. It provides this service against payment after being hired by the Election Host. The voters take part in the election using the VSP's voting service. The public is allowed to witness the election procedure for the purpose of verification.

We specify the VSP's function more clearly. The goal of the VSP is to provide the secure technical implementation of online elections. To this end the VSP participates in the election procedure and takes on the technical implementation of all tasks required for a secure online election on the part of the operator. The VSP provides the secure online voting software and the secure operational environment. It takes care of secure processes throughout at least the preparation, the voting and the tallying of the online election. The specific tasks follow from the election processes and the corresponding legal and technical security requirements. The VSP provides the expert knowledge that is required to securely operate the online election. Therefore it employs skilled personnel which is qualified to configure, to run and to maintain the online voting system.

The VSP acts as the executive power on behalf of the Election Host. It does not affect the Election Host's legal responsibilities. While the VSP handles the technical implementation it does not take on the superior tasks of the Election Host, like for example setting the election dates and drawing up the list of candidates, or typical tasks of the election board like initiating the voting or tallying phase. The specific allocation of tasks might be laid down in a service level agreement. We consider the case of a VSP that takes on as many tasks as possible. This is in particular plausible since the VSP intends to take on the necessary efforts and enable efficient online elections.

2.2. Processes

Next we outline how an election takes place and which tasks can be taken on by the VSP. For this purpose we summarize the most common election processes following current literature on electronic voting (see [41, 93, 30, 96]) as well as legal regulations for federal and state elections in Germany (see [7, 16, 19]). Then we transfer these processes to the VSP scenario and consider the contribution of the VSP.

Pre-voting phase According to the literature this stage is primarily concerned with the registration of voters. The identity and eligibility of the voters is determined and the electoral roll is created (see [41, 93, 30], [16, §§14–24], and [7, §17]). Next the electoral roll and additional election data like for example the candidates list, the timetable, and

the ballot representation are announced publicly (see [30, 93], [16, §20, §38, §43, §48], and [19, §§2–3]). Based on those parameters the voting system is set up [30].

Now we consider which of those processes can be taken on by the VSP. The VSP realizes the registration of voters by technical and organizational means. For example the VSP provides a website where the voters prove their identity using their electronic ID card. The Election Host transmits further election data to the VSP, for example the list of candidates, the election dates, the electronic ballot representation, or the election regulations. The VSP publishes selected election data on a specific website for election announcements. Next the VSP uses the transmitted information to set up its voting system accordingly. It installs and configures the software and the hardware of the voting system to meet the specifics of the current election scenario.

Voting phase In this stage the election is opened and the eligible voters start casting their votes after prior authentication (see [93, 41, 30] and [16, §53, §56]). Especially in electronic voting the voters are allowed to verify the correctness of the voting procedure [96]. This depends on the voting scheme in use. According to the election schedule the voting phase is closed after a specified time frame and no further votes are accepted.

Next we look at the VSP scenario again. The VSP can take on many tasks at this stage. It opens the election by starting the corresponding application on his website. This step might be initiated by the Election Host in order to retain his superior responsibility for the election. In this case the VSP provides a specific website for the Election Host that allows him to access the voting system and initiate the voting phase. The voters authenticate themselves and cast their votes via their computer or mobile device at the VSP's voting website. Depending on the voting scheme the voters use specific credentials like PINs or TANs for authentication or voting purposes. The VSP delivers those credentials in advance. For verification the VSP makes the particular functionality of the voting scheme available to the voters, for example to allow for individual verification that the vote has been cast as intended. At the end, the VSP closes the election by terminating the vote casting process. Again this step might be initiated by the Election Host using the VSP's corresponding website.

Post-voting phase After all votes have been collected the tallying is started (see [93, 41, 30], [16, §69], and [19, §§13–14]). The election result is published ([93, 30], [16, §70, §79], and [19, §18]). Many electronic voting schemes provide the functionality to verify the correctness of the election outcome [93, 41, 30]. In classic elections voters are allowed to observe the counting procedure for this purpose (see [16, §54] and [19, §13]).

Those tasks are transfered to the VSP in the following way. The VSP starts the tallying procedure of his voting system. This step might again be initiated by the Election Host using a specific website provided by the VSP. After counting all votes the VSP publishes the election result using an information website that is accessible for all authorized persons. The VSP enables the voters and the public to universally verify that all votes have been counted correctly. For example, the VSP provides the collected votes on his website together with suitable tools for reproducing the tallying by oneself.

To ensure an independent verification procedure such auditing tools could be provided by independent entities instead.

2.3. Architecture

We describe the very basic components that a VSP uses to implement an online election. To this end we identify which components are required in the processes we introduced before. We present an overview in Figure 2.2 and provide further details in the text where we consider the hard- and software as well as structural components of the VSP.

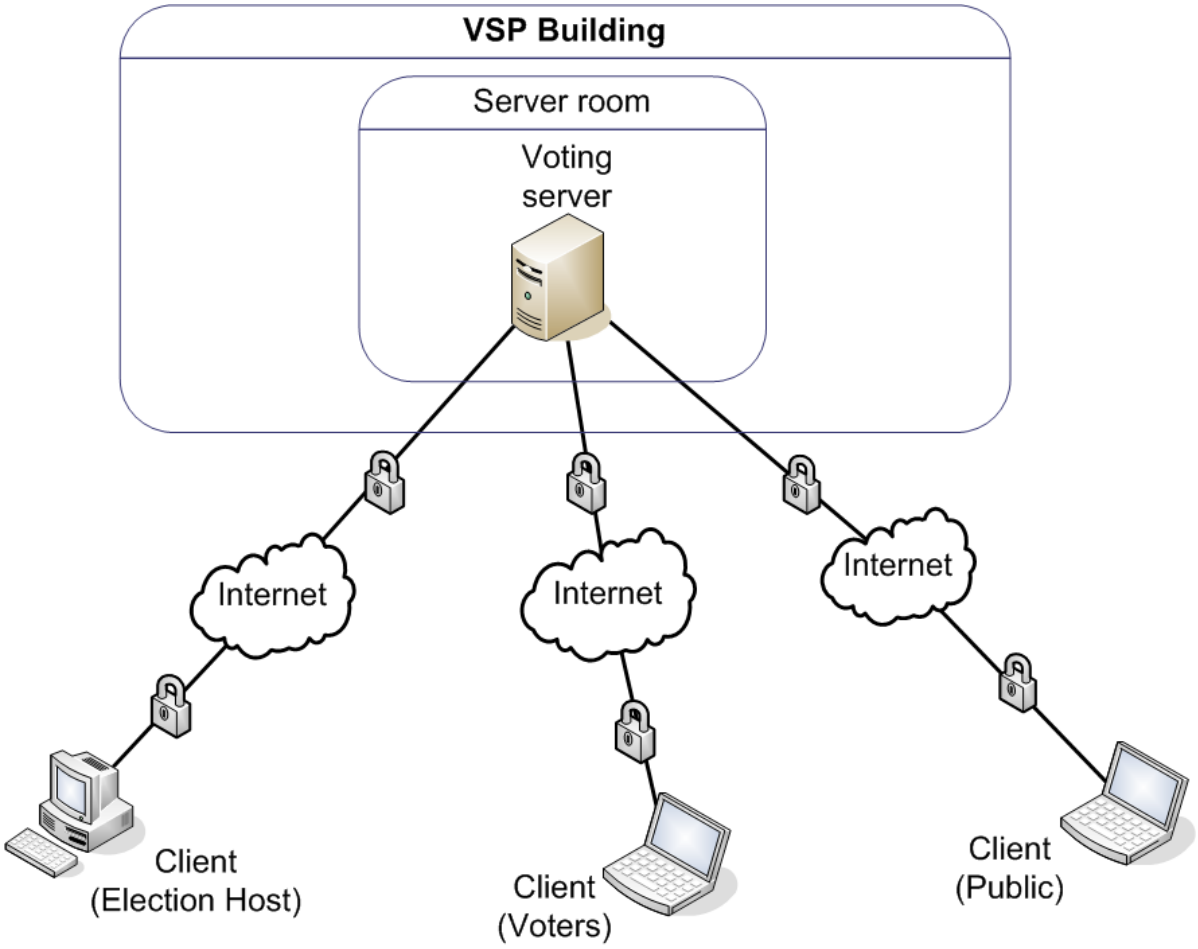

Figure 2.2.: VSP Architecture

We assume that in general the VSP is an external service provider that is located in a secure building of its own, possibly a computer center. The server-sided voting system is located in protected server rooms. The processes suggest that the VSP sets up the voting service as an Internet portal which provides specific websites for all participants of the election corresponding to the user's role. After successful authentication at the Internet portal the users can access corresponding data and execute related tasks using

their terminal devices. While the voters hereby cast their votes, the Election Host is enabled to submit required election data or execute administrative tasks. This is a typical use case for a client-server architecture. The specific components depend on the voting scheme in use. We therefore describe a simplified client-server architecture with one server that combines all potential server-sided functions. Real implementations might vary at some points. For example there could be several dedicated servers, each for a single task like for example collecting the votes or counting the votes.

The voting server runs the voting software. It is set up as a web server with appropriate standard software. To store identification and authentication data of the voters and finally the electronic votes the server has a database installed to manage such data. Where necessary, the server-sided system components are connected via an internal network to interchange data. The specifics of these network links depend on the requirements of the voting scheme in use. They range from standard LAN connections to highly secure air-gapping channels where data is transferred by hand on memory devices. Moreover the internal network includes standard components like security gateways or routers and switches that interconnect the internal network with the Internet to enable access for the voters, the Election Host and the public. These parties connect to the VSP's voting system over the Internet using secure communication channels. These channels are based on standard protocols like SSL to provide a high level of compatibility for a wide range of terminal devices. The voters, the Election Host and the public use such client devices to cast votes, to execute administrative tasks or to look up the election result. Depending on the voting software, possible terminal devices might be PCs or cell phones. We do not consider the client devices part of the VSP.

2.4. Properties of the VSP Concept

The VSP concept introduces some unique features for realizing secure online elections. We outline the most important properties and consider the potential advantages. By outsourcing the technical implementation to a VSP, the effort of carrying out a secure online election is reduced for the Election Host. For example, the Election Host does not need to provide the secure operational environment nor the expert knowledge to configure the voting system. This might make online elections more attractive for the Election Host. Furthermore, a single VSP can use its online voting service to implement many elections for various Election Hosts. Hence the required online voting software and the operational environment only need to be provided once. This might reduce overall costs. This is particularly plausible for non-political election scenarios where elections take place more frequently, for example the elections of works councils in companies. Here the VSP concept would represent a potential business model which might even stimulate business interest in the realization of secure online elections.

Next we consider those aspects of the concept that promise to enhance the security of online elections. The VSP is a qualified service provider and thus professionalizes the implementation of secure online elections. It uses well-approved and tested technology and skilled personnel. Implementing many elections as a business, the VSP provides

experience and expert knowledge. The concept allows addressing the security of online elections from a new perspective: the VSP accommodates the online voting software and the operational environment. This centralized approach facilitates regulation as well as overall evaluation, certification and accreditation. While a regulatory framework would clearly define the requirements for secure online elections, a corresponding evaluation, certification and accreditation concept would verifiably ensure that these requirements indeed are satisfied by the VSP. A combination of these ideas might increase the security of online elections. We will introduce a corresponding approach to enable secure VSPs in the next chapter.

3. Security Approach

In this chapter we describe an approach to make online elections with Voting Service Providers (VSPs) secure. To this end we derive the necessary building blocks and introduce suitable methodologies to implement them. We will address these building blocks in the following chapters. This chapter is based on work we published in [P1] and [P2].

3.1. Requirements

As an overview we first illustrate the security approach in Figure 3.1 and outline the methodical steps in Figure 3.2. In the following text, we describe the single building blocks (denoted in *italics*).

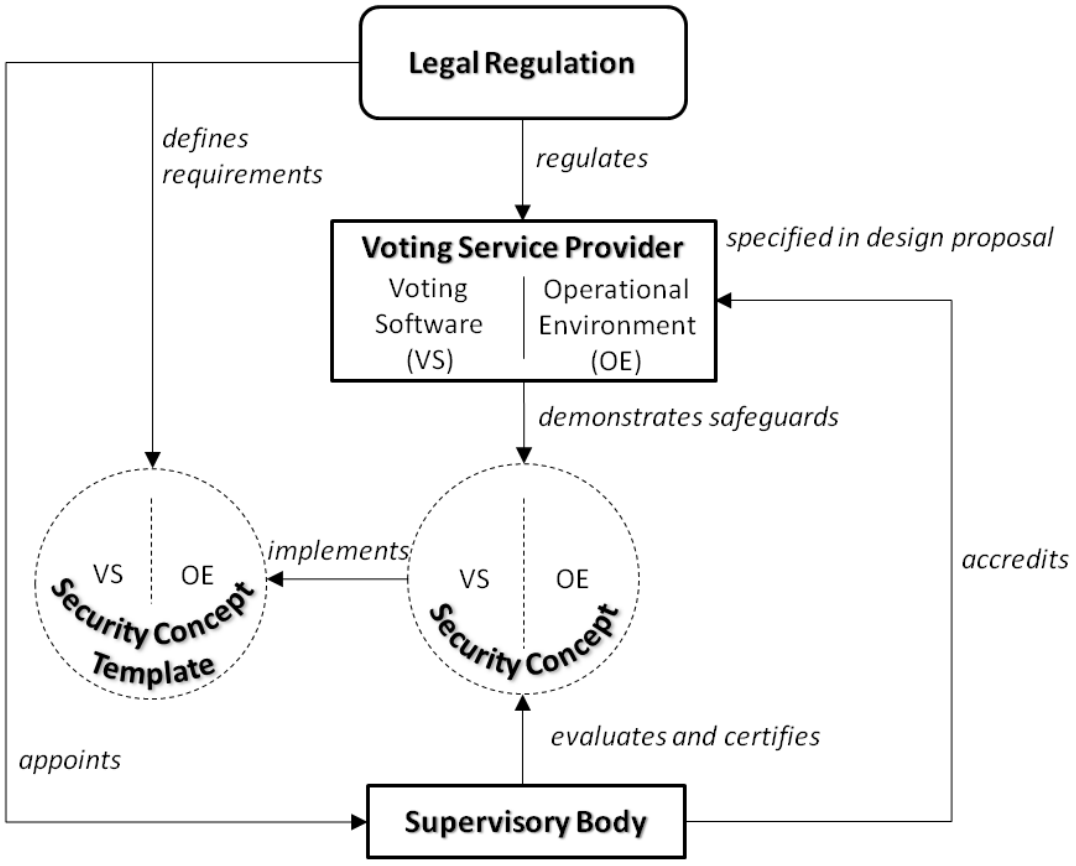

Figure 3.1.: Security Approach

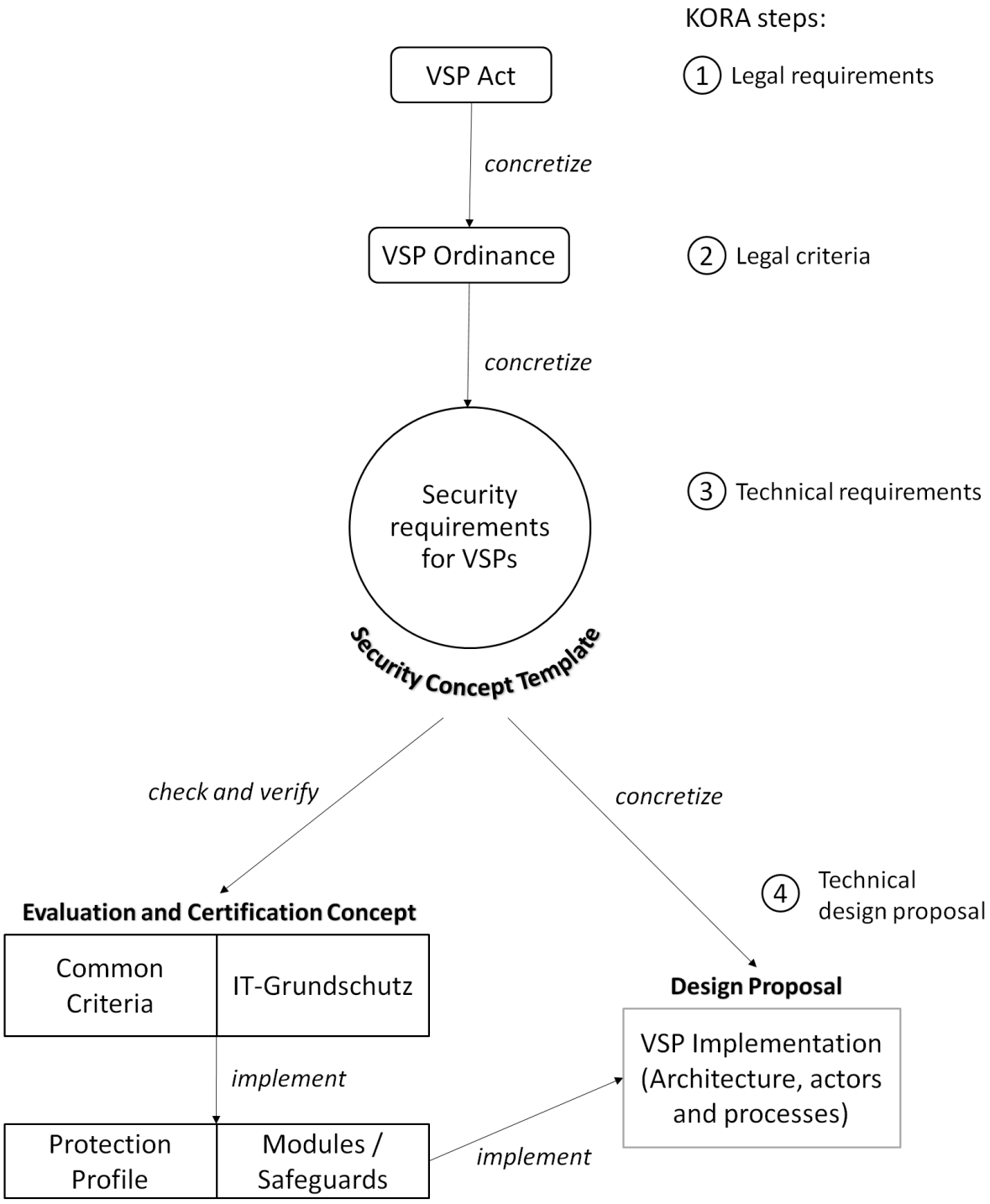

Figure 3.2.: Methodology

First of all, the VSP has to fulfill the requirements for secure online elections. To this end a *legal regulation* defines the requirements for secure online elections with VSPs. This is reasonable because elections need to observe the basic democratic principles and

therefore are legally regulated. The same has to apply to online elections. Furthermore, such legal regulation is necessary to enable legally binding online elections with VSPs. The legal regulation of security-critical IT service providers has proven successful in the similar scenario of Certification Authorities (CAs) in Germany. The requirements for their operation are defined in the German Electronic Signature Act and the corresponding ordinance (see [102, 103]). However legal requirements are rather abstract and general. To comply with the legal regulation, the VSP needs clearly specified technical requirements that enable him to implement suitable safeguards. Therefore we derive corresponding technical requirements from the legal regulation and list them in a *Security Concept Template*. It contains the technical requirements for the VSP's online voting software and its operational environment.

A suitable methodology to derive the requirements is KORA[1] (see [72] for an introduction). It identifies legal requirements and concretizes them in several steps to make them technically usable. KORA has been successfully applied many times for IT products and services (see [73, 84, 74, 106, 77] for examples). In the first step, "legal requirements" are identified based on the first part of the legal regulation, the VSP Act. In the second step, the previous results are concretized to "legal criteria". They describe problem solutions for the legal requirements on an abstract level without providing a specific technological approach (cf. [72]). This step is based on the second part of the legal regulation, the VSP Ordinance. In the third step, "technical requirements" are derived by incorporating technical input like technical standards or requirements catalogs to further concretize the legal criteria. The technical requirements serve as the basis for a technical implementation. This step is addressed to develop the Security Concept Template.

3.2. Verification

Now that the requirements are set it has to be verified that the VSP effectively satisfies them. This is realized by an *evaluation, certification and accreditation* procedure. Only the resulting verification definitively guarantees the security and thereby generates the necessary trustworthiness of the VSP towards the Election Host and the voters. This approach has been generally accepted and is used in many areas, in particular in the similar CA scenario. In our VSP security approach the procedure is regulated in the legal regulation. It appoints a Supervisory Body that thoroughly evaluates the VSP based on its Security Concept. In this document the VSP demonstrates that he satisfies the technical requirements for the voting software and the operational environment. In case of a positive result the Supervisory Body certifies the VSP's legal compliance. Then the Supervisory Body accredits the VSP to announce officially that it provides online voting services that comply with the law. This procedure has proven successful in the similar CA scenario in Germany where it is regulated in the Electronic Signature Act [102].

[1] KORA (KOnkretisierung Rechtlicher Anforderungen, engl.: Concretizing legal requirements)

To realize the evaluation and certification of a VSP suitable methodologies need to be used. We demonstrate the applicability of the following methodologies. For the voting software, we propose the Common Criteria for Information Technology Security Evaluation. It is an international standard (ISO/IEC 15408) for the evaluation and certification of security-critical software and hardware components [42]. Common Criteria has already been applied to the field of online voting. The "Common Criteria Protection Profile for Basic set of security requirements for Online Voting Products" is a current standard for the evaluation and certification of online voting software [64]. It is in particular suitable for the VSP scenario since it focuses on non-political elections. For the evaluation and certification of the operational environment we propose the IT-Grundschutz methodology (engl. IT Baseline Protection) that is developed and maintained by the German Federal Office for Information Security [62, 66]. IT-Grundschutz provides an approach to ensure the security of complex IT infrastructures which consist of infrastructural, organizational, personnel and technical components. To this end, IT-Grundschutz includes a comprehensive catalog of modules and safeguards (see [59]) which can be implemented in order to satisfy the protection requirements. In order to prove the achieved security level IT-Grundschutz includes an evaluation and certification methodology. IT-Grundschutz is compatible to the international ISO 27001 standard and incorporates its evaluation methodology [22]. ISO 27001 specifies requirements for introduction, operation and improvement of information security management systems (ISMS) [80]. It is already in use in the electronic voting context: A Swiss project in Geneva is working on the implementation and evaluation of an electronic voting system[2] which is planned to be evaluated according to ISO 27001 [21, 107]. IT-Grundschutz enhances this methodology with its multitude of safeguards and a predefined risk assessment that reduces the evaluation effort.

As a result we obtain a *design proposal* for the VSP in accordance with the fourth step of the KORA methodology. We use the identified safeguards and demonstrate how they can be used to implement a VSP. This verifies the feasibility of the VSP concept in practice.

[2] `http://www.ge.ch/evoting/english/welcome.asp`

4. Legal Regulation

As the first building block of our security approach we describe the legal provisions for Voting Service Providers (VSPs). To this end we first introduce a legal regulation for VSPs. It consists of an act and an ordinance. Then we identify the legal requirements and derive their first refinement, the legal criteria, by applying the KORA methodology. They serve as the basic security definition that we will develop further in the next chapters. Finally, we discuss certain questions regarding the application of the legal regulation, current jurisdiction and its relevance for our work, as well as the applicability of the legal regulation to different election scenarios. The legal regulation for VSPs provides the basis for secure and legally binding online elections. It has been developed by an interdisciplinary circle of experts in technical law and electronic voting led by Prof. Dr. Alexander Roßnagel, University of Kassel, within the project "voteremote" which was funded by the German government (see [P10] for details). The author of this thesis was a member of this circle and contributed to the development from the technical perspective. This chapter is based on work we published in [P3] and [P6].

4.1. The VSP Act

The VSP Act regulates the operation and the accreditation of VSPs and their online voting services[1]. The regulation is designed for non-political election scenarios. Thereby it provides a foundation for future legal regulation for other election scenarios to build on. In this section we introduce the most relevant contents of the VSP Act in a brief summary[2]. The complete VSP Act contains additional regulations on fines for illegal behavior of VSPs and provisions on charges the VSPs may levy. Details can be found in our publication [P3], the complete text is available in [92].

The VSP Act assures compliance with constitutional and other legal regulations. To this end applicable laws have been considered in its development. First, general provisions regarding the democratic participation from the German constitution ("German Basic Law") have been observed [3]. Regarding specific electoral law, the German Works Constitution Act for the context of non-political elections has been taken into account [11]. Since the VSP handles sensitive data, the German Federal Data Protection Act has been incorporated [6]. Furthermore, the German Teleservices Act has been considered

[1] For the sake of generality, the original wording in the legal regulation for VSPs is "remote electronic election" and "remote electronic voting" [92]. Instead, we use the terms "online election" and "online voting" respectively to maintain a consistent wording throughout the thesis.

[2] Parts of this section can also be found in our publication [P3] with minor textual changes.

[10]. It regulates the liability of telemedia[3] service providers, the handling of data in telemedia services and the responsibility of the service provider for the contents of its telemedia service. At last, the German Electronic Signature Act, especially its structure, has been examined due to the similarities of the Certification Authority (CA) scenario (see Chapter 3 and [102] for details).

Part 1 – General Provisions

Purpose, Scope and Terminology Purpose of the statutory approach is to create a legal regulation for certified trustworthy online voting services. The act does not preclude offering similar services without certified trustworthiness. The framework does not concentrate on specific elections but on the service of providing online elections for different non-political types of elections. An "online election" is an electronic election in which the voter is able to cast his/her vote using a networked terminal device. A "VSP" is everyone providing online voting services for business.

Part 2 – Accreditation

Voluntary Accreditation of VSPs In this article the act introduces the accreditation as a means to promote trust in the VSP and its election procedure. It assures evaluation and certification of compliance with basic election principles, technical and organizational security and data protection. Generally, accreditation means that a VSP has provided reliable proof of verified trustworthiness of its services. For this, a VSP has to apply for an official certificate. An administrative authority, the Supervisory Body, will be responsible for evaluating, certifying and accrediting the VSP. The Supervisory Body may employ private services to perform the evaluation and certification process, thereby reducing administrative effort. Accredited VSPs will be issued a certificate by the Supervisory Body. They may then carry the title "Accredited VSP" to indicate their compliance with the legal regulation and thereby their trustworthiness. To continually ensure this, a repeat accreditation process is mandatory every three years or earlier in case of severe security relevant changes to technology or organization. If a VSP does not fulfill the obligations imposed by the act or the corresponding ordinance or if an accreditation requirement is no longer fulfilled, the Supervisory Body will revoke the accreditation. The act does not preclude non-accredited VSPs from offering similar services. This assures conformity with article 12 of the German Constitution [3]. Consequently, the accreditation procedure is fully voluntary. However, there are several reasons and incentives to become accredited: Other laws may prescribe accreditation for a specific type of election. Also, employing an accredited VSP can facilitate and professionalize online elections. This can create market demand for accredited VSPs. The act leaves rights and duties of the Election Host untouched.

Accreditation Requirements The act defines the legal provisions that a VSP needs to comply with in order to be accredited. For example, this includes the reliability and

[3]The term "telemedia" refers to Internet-based information and communication applications.

specialist qualification necessary for the operation of a VSP, particularly regarding the personnel. Moreover a VSP will only be accredited if it fulfills the legal obligations concerning the election principles, the technical and organizational requirements for the operation of an online election, as well as the briefing and the documentation in a way that ensures secure and reliable online voting services. Additionally, accreditation requires the VSP to operate in accordance with the legal provisions on data protection.

Proof of Accreditation Requirements In this article the act defines how a VSP is supposed to demonstrate its compliance with the legal provisions for accreditation. The reliability and specialist qualification of the VSP's personnel must be proven by suitable certificates. The satisfaction of all technical and organizational requirements is to be demonstrated in the 'Security Concept' of the VSP (see Section 4.2). It has to be evaluated and certified with respect to its suitability and practical implementation by the Supervisory Body or respective recognized authorities. The evaluation examines the VSP's software, hardware as well as technical and organizational security for their compliance with the legal provisions. Evaluation of deployed technical products or other specific parts of the Security Concept can be omitted if their security is proven by means of an approved security certificate. In addition, fulfillment of the data protection provisions must be certified by an authority recognized by the Supervisory Body.

Recognition of Foreign Services Comparable services from another member state of the European Union or from another contracting member state of the Treaty on the European Economic Area are, concerning their legal consequences, treated as equal to the services of an accredited VSP if they provide equivalent trustworthiness that is certified by a suitable authority of this member state and if the continuity of trustworthiness is ensured by means of existing control measures in this state.

Part 3 – Legal Obligations of the VSP

Election Principles A key component to achieve trust in the voting process is for the VSP and its online voting service to comply with the basic election principles to an extent defined by the requirements of the particular type of non-political election. Basically the VSP has to ensure at least the availability, the confidentiality and the integrity of the online election as well as the secure identification and authentication of the voters. We point out the security of online elections here is summarized in the election principles and basic requirements. Satisfying these principles means in consequence to achieve the known security objectives of electronic voting. Hence these objectives do not need to be mentioned in the law directly.

Performing an Online Election Next the act states in more detail which legal obligations the VSP has to observe during the implementation of an online election. For example, to reliably identify eligible voters and candidates the accredited VSP has to use respective registers of persons entitled to vote and persons with the right to stand

for election. The Election Host is responsible to create and deliver such registers to the VSP. The Election Host generally remains responsible for the voting process while the VSP is responsible only for the technical and organizational implementation. Therefore the VSP has to enable the Election Host to perform certain control tasks like starting and stopping the election or initiating the counting of votes at its will. Furthermore, the act defines how the VSP has to implement the vote casting. This includes prior identification and authentication of the voters, complete and equal display of the voting options, as well as the necessary steps to cast a vote and to verify its storage. The act requires the VSP to ensure a correct and verifiable counting of votes that protects the secrecy of the voters. At last, the act stipulates that the VSP documents all essential actions of the online election and protects the record from unauthorized access.

Briefing Obligation In order to increase the overall election security, the act requires the VSP to brief all actors that operate outside the VSP's area of responsibility, that is the voters and the Election Host, on remaining security risks and on the measures they have to take care of.

Documentation Obligation In this article the act provides further regulations regarding documentation data, their protection as well as their handover to the Election Host.

Part 4 – Supervision

Responsible Authority To ensure legal compliance and a standardized security level of online voting services, the operation of VSPs is controlled by a federal authority, the Supervisory Body. Its responsibilities include accreditation and supervision of the VSPs.

Recognition of Evaluation and Certification Authorities The Supervisory Body recognizes a private party upon application as evaluation or certification authority according to the VSP Act, if this party proves the reliability, the independence and specialist qualification necessary for the activity. The recognized authorities have to fulfill their duties impartially, autonomous and conscientiously. Moreover they have to document the evaluations and certifications and hand the documentation over to the Supervisory Body in case of abandonment of their practice.

Measures of Supervision The Supervisory Body supervises observation of act and ordinance. It may employ private subsidiaries for performing the supervision. To perform its duties the Supervisory Body is authorized to enforce measures towards VSPs as well as the evaluation and certification subsidiaries it employs. The Supervisory Body prohibits a VSP or an evaluation or certification subsidiary from conducting business temporarily, partially or entirely, if the prerequisites for accreditation or recognition are no longer fulfilled, unsuitable products are used or obligations are violated. Finally, the Supervisory Body provides names, addresses and other contact data of currently and formerly accredited VSPs to the public.

Co-operation Obligation In order to support the Supervisory Body in performing its duties, VSPs as well as evaluation and certification authorities are required to grant the Supervisory Body access to their offices, present documents, protocols and further records for insight on demand, and give information and necessary support.

4.2. The VSP Ordinance

The VSP Ordinance provides details and additions to concretize the regulation given in the VSP Act[4]. This allows the regulation to be adapted to new scenarios and techniques more easily. The ordinance keeps the act free from details and allows quick reaction to legal or technical changes. Separating act and ordinance is necessary, because legal regulations made by acts are intended to be valid long-term and apply to many scenarios. Passing an act is a complex process and thus changes to the final act are to be avoided. Consequently, acts are restricted to general rules and regulations. This is solved by introducing a separate ordinance to be passed by executive order. To specify the details and additions in the VSP Ordinance the German Electronic Signature Ordinance has been taken into account because the similar context, in particular the evaluation, certification and accreditation procedure for CAs, allows various aspects to be adapted to the VSP Ordinance (see [103]). As before we present a summary of the most relevant parts of the VSP Ordinance. The complete version includes additional provisions on the verification of product suitability, on the procedure for recognition of evaluation and certification authorities and on the assessment of charges. Details can be found in our publication [P3], the full text is available in [92].

The Security Concept Its Security Concept is the basis for the evaluation, certification and accreditation of a VSP. The VSP has to demonstrate all measures taken to assure compliance with the legal regulation. Thus, the Security Concept must contain the following descriptions: all necessary technical, constructional and organizational security measures and their suitability, the technical products used for the online election, the organization of setup and process, compliance with the election principles, with data protection acts and of measures for ensuring and maintaining operation, especially in case of emergencies, the procedures for evaluating and ensuring the reliability of the deployed personnel and an estimation and validation of remaining security risks. To sum up, the Security Concept includes all security relevant aspects of the VSP's voting system and its operational environment.

Requirements for Performing Online Elections In this article the ordinance specifies provisions for the technical and organizational implementation of the election procedures. We provide some examples. First it elaborates on the extent of availability that the voting service must ensure. This includes instructions how to deal with system interruptions and restarts. Next, the ordinance contains additional provisions on the secure

[4]Parts of this section can also be found in our publication [P3] with minor textual changes.

delivery of authentication means, the secure transmission and storage of data during the election processes, or the electronic ballot layout. Furthermore it demands the secure initial state of the voting system, that means for example an empty ballot box. The necessary steps of the voting procedure are defined, in particular the options for the voter to correct the voting decision, to interrupt the process without losing suffrage or to receive a confirmation for voting. Further details are added how to securely suspend and terminate the voting procedure. For example, after closure of the voting phase, vote casting already in progress must be allowed to finish within a predefined period. At last, the ordinance provides details on the counting procedure that is to be initiated by the Election Host, and the publishing of the results.

Extent of Documentation The VSP Act requires the VSP to document certain actions and events during the election procedure. The VSP Ordinance now adds provisions regarding the archiving of such data. This includes requirements on the readability outside the voting system, in particular to allow recounting the electronic votes by arbitrary tallying software to provide transparency and verifiability of the tallying procedure. Moreover the ordinance stipulates the protection of the archived election documentation by suitable technical means.

Arrangement of Briefing While the VSP Act requires the VSP to brief the Election Host and the voters on particular tasks and safeguards, the VSP Ordinance now defines the contents of this briefing. Regarding the Election Host, it includes for example the security and compatibility of the terminals devices, the measures which have to be implemented by the Election Host, and the remaining security risks. The briefing for the voters comprises instructions on the technical steps leading to casting of a vote, on the secure communication with the voting system of the VSP, and on the necessary security precautions on the terminal device used for the online election. For example, the VSP must inform about risks resulting from malicious software like viruses and how to protect the terminal devices against this threat.

4.3. Legal Requirements and Legal Criteria

In this section we present the *legal requirements* that a VSP needs to satisfy for compliance with the introduced legal regulation. To this end we analyze the VSP Act given in [92] to identify the contained legal requirements. They were derived from constitutional and other applicable law during the development of the VSP Act (see Sections 4 and 4.1 for details), thereby implementing the first step of the KORA methodology (see Chapter 3 and [72] for an introduction). Then, to concretize the abstract legal requirements, we follow the second step of the KORA methodology and derive *legal criteria*. While still non-technical, the legal criteria add further details and specifics how to fulfill the legal requirements. To identify such additions we analyze the corresponding articles of the VSP Ordinance and the explanatory memorandum of the VSP Act given in [92].

While the VSP Ordinance contains more detailed regulations, the explanatory memorandum provides information on the background, the intention and the reasoning of the specific provisions of the VSP Act. The explanatory memorandum thereby helps interpreting the VSP Act in the intended way. For our work we used the full text of the legal regulation. It also includes the explanatory memorandum and is available in [92]. Since the full text is in German language we translate the relevant passages that we use for the legal requirements and the legal criteria into English. At last, we identify the basic election principles that are affected by each legal criterion. We will make use of this classification to further concretize the legal criteria in the next chapter. To do so we refer to the definitions given by Volkamer [109, p. 61]. We list the election principles in Appendix A.2 for reference.

The legal requirements for VSPs are spread over the articles of the VSP Act. However the relevant articles are listed in article §4 of the VSP Act which regulates the accreditation of VSPs. For the first requirement we therefore start with article §4 (1) and identify the following regulation concerning the VSP's personnel.

Legal Requirement 1. *Accreditation requires the reliability and specialist qualification necessary for the operation of a VSP. A VSP is reliable if it guarantees observation of the legal provisions regarding its operation. It has the necessary specialist qualification if its personnel have the knowledge, experience and skills necessary for this activity.*

We derive the following two refinements.

Legal Criterion 1.1 (all)**.** *The VSP must implement procedures for evaluating and ensuring the reliability of the deployed personnel. The reliability necessary for operation normally is proven by means of up to date certificate of good conduct according to the Federal Central Criminal Register Act §30 (5) [5]. The specialist qualification necessary for particular tasks during operation is proven by means of respective certificates which prove that the qualification for the particular job specification is sufficient.*

Legal Criterion 1.2 (all)**.** *The VSP must provide an estimation and validation of remaining security risks.*

Both criteria are based on additional information given in VSP Act §5 (1), the corresponding article in the explanatory memorandum, as well as VSP Ordinance §1. In their generality, they affect all election principles and are therefore classified (all).

Next, VSP Act §4 (2) requires accredited VSPs to satisfy the obligations described in §§7–11.

Legal Requirement 2. *The VSP must provide online services which fulfill the requirements applying to the implementation of the particular election. The online voting services shall be permanently available during the voting period. They must ensure security and confidentiality of the election as well as identification and authentication of the voters. They must reveal alteration of voting documents.*

This requirement is given in VSP Act §7. We find the following corresponding legal criteria.

Legal Criterion 2.1 (un)**.** *The VSP must ensure by means of suitable measures that the communication and voting system is available during at least 95% of the election period and that it enables counting of votes after the end of the voting process.*

Legal Criterion 2.2 (un, di)**.** *Upon interruptions the voting system must ensure a secure restart sustaining the legal election principles and saving the votes already cast and all necessary data present before interruption.*

These refinements are based on VSP Ordinance §3 (1). As noted in the explanatory memorandum of the VSP Ordinance they affect the basic principle of an *universal* election (un) since the availability of the voting system is a prerequisite for each voter to participate in the election. The second criterion additionally affects the principle of a *direct* election (di) because it adds to determining the correct election result based on all cast votes.

Legal Criterion 2.3 (un, tr)**.** *The VSP shall implement precautions to guarantee and maintain the operation of the online voting service according to the legal regulation, especially in case of emergencies.*

This criterion results from VSP Ordinance §1. It additionally affects the principle of *trust* (tr) since it adds to maximizing public trust in the election robustness.

Legal Criterion 2.4 (un, fr)**.** *The online voting system must transmit, receive and store identification data of the voters and votes protected from unauthorized disclosure.*

Here, VSP Ordinance §3 (1) refines VSP Act §7, sentence 3. It affects the principle of an universal election since it protects the identification data required to identify all eligible voters. Furthermore it addresses the principle of a *free* election (fr) because disclosed data transmission or storage might endanger voter's free voting decision. For example, an attacker might compute and publish intermediate results.

Legal Criterion 2.5 (eq, un, di)**.** *The VSP must accomplish identification and authentication of the voter by use of at least two independent securing means. It must ensure confidential and unaltered handover to the voter's power of disposition. The VSP must ensure that upon correct usage of the securing means, casting of a vote by individuals not eligible to vote or casting of multiple votes by individuals entitled to vote is prevented.*

This criterion is picked up again in VSP Act §8 (3) (see Legal Requirement 5) and refined in VSP Ordinance §3 (3). Authenticating the voter is required in order to check whether a voter already has cast a vote or not. Therefore this criterion adds to the principle of an *equal* (eq) election. Checking the voter's eligibility supports the principle of an universal and direct election.

Legal Criterion 2.6 (di, un, tr)**.** *The voting system must be able to detect unauthorized modification, erasure and addition of identification data of the voters, votes, protocol data and further relevant data. Alteration of election data must be recognizable at any time, their authenticity must be verifiable.*

Here, the explanatory memorandum of the VSP Act as well as VSP Ordinance §3 (1) refine the fourth sentence of VSP Act §7 by indicating more clearly the type of data to be protected as well as the protection goals. By addressing the protection of identification data and votes, this criterion affects the principles of a direct and universal election. The aspect of verifiability adds to the principle of trust.

Next, we address the requirements given in VSP Act §8. This section of the legal regulation considers the implementation of the online election.

Legal Requirement 3. *The VSP must take over the registers of persons entitled to vote and persons with the right to stand for election from the Election Host for use in the online voting service.*

We identified this legal requirement in VSP Act §8 (1). It can be refined as follows.

Legal Criterion 3.1 (di)**.** *The VSP must take over the registers of persons entitled to vote and persons with the right to stand for election from the Election Host for use in the online voting service. The lists are transmitted in written or electronic form, the VSP must transfer them into the voting system correctly and reliably.*

The criterion is derived from the information given in the corresponding article of the explanatory memorandum of the VSP Act. It is a precondition for identifying all eligible voters and thereby helps to gather all votes correctly. Thus it adds to the principle of a direct election.

Legal Requirement 4. *The VSP must enable the Election Host to initiate, to suspend and to terminate the online election and to initiate the counting of votes.*

This requirement originates from VSP Act §8 (2). We identify several refinements.

Legal Criterion 4.1 (–)**.** *The VSP must enable the Election Host to initiate and to terminate the online election. It must ensure that in case of technical malfunction and other emergencies, the Election Host is able to interrupt the online election. After positive identification and authentication the VSP must enable the Election Host to initiate the counting of votes.*

The first refinement is derived from the articles §3 (2) and §3 (6) of the VSP Ordinance. It only addresses the allocation of obligations and responsibilities in the scenario of an online election with a VSP. Thus it does not affect the basic election principles.

Legal Criterion 4.2 (di)**.** *Directly before starting the voting procedure, the VSP must enable the Election Host to verify that the ballot box does not contain any votes and that all other parts of the voting system are in their predefined initial state.*

This refinement from article §3 (2) of the VSP Ordinance elaborates on the initiation of the election. It ensures the counting only of eligible votes and therefore affects the principle of a direct election.

Legal Criterion 4.3 (un)**.** *After closing of the voting, the VSP must allow voting procedures already in progress to be completed within the time limit set before starting the election by the Election Host. After expiration of the time limit, further voting procedures, voting related transmissions, acceptance of further votes and restarting of the online voting system must not be possible.*

This criterion also originates from additional information given in article §3 (2) of the VSP Ordinance. It is assigned to the principle of an universal election since it supports each eligible voter to cast his vote.

Legal Requirement 5. *The VSP must display the existing voting options completely and equivalently to the voters, allow the voters to abort the voting procedure, to make, to correct and to cast a voting decision and to verify the storage of the vote.*

This legal requirement is given in VSP Act §8 (3). (The first sentence on identification and authentication of the voters is already addressed above in Legal Criterion 2.5). We identify the following criteria.

Legal Criterion 5.1 (fr)**.** *The VSP must display the whole content of the electronic ballot in a reasonable discernible manner. The VSP must grant the same space for each voting option and implement the representation options as requested by the Election Host corresponding to election specific legal provisions. If polling booth voting or absentee voting is available as alternative voting channel, the representation of both the electronic ballot and the paper ballot must be equivalent.*

Here, VSP Ordinance §3 (4) provides specific information to refine the legal requirement. The refinement addresses the effect of the ballot representation on the voter's voting decision and is therefore related to the principle of a free election.

Legal Criterion 5.2 (fr, un, tr, se)**.** *The VSP must ensure that the voters*

1. *are able to make and to cast a voting decision (fr, un),*
2. *are able to cast an invalid vote (fr),*
3. *are able to abort the voting procedure without losing elective franchise (fr),*
4. *are able to correct their vote any number of times until the final voting (fr, tr),*
5. *receive a confirmation for their voting and are able to verify the storage of the vote (fr, tr),*
6. *are not enabled by the voting system to show their voting decision to others (fr, se).*

The foregoing refinement is derived from VSP Ordinance §3 (5) which provides more details regarding the particular steps of the voting procedure. The particular items contribute to the election principles noted in brackets.

Legal Requirement 6. *After completion of the election, the VSP must ensure a correct counting of votes verifiable at any time.*

This legal requirement represents §8 (4) of the VSP Act. It has the following refinement.

Legal Criterion 6.1 (di, tr)**.** *The software used for counting must ensure the correct counting of votes and that the single steps can be verified and reproduced at any time afterwards. The integrity and completeness of the votes intended for tallying must be ensured by technical means that allow for their verification. The counting must be initiated publicly in the premises of the Election Host and the result must be published. It must calculate the number of all valid and invalid votes that have been stored in the electronic ballot box after completion of the ballot casting. It also has to determine the proportion of votes each ballot option received.*

This refinement originates from the corresponding article §8 (4) of the explanatory memorandum of the VSP Act, as well as from VSP Ordinance §3 (6). They add details regarding the tallying procedure. The criterion affects the principle of a direct election since it addresses the correct counting based on all votes of eligible voters. The verifiability aspect enhances the transparency and thereby adds to the principle of trust.

Legal Requirement 7. *The VSP must record all essential actions of the online election and protect the record from unauthorized access. Immediately after completion of the election, the accredited VSP must hand the election protocol over to the Election Host.*

This legal requirement represents VSP Act §8 (5) and §10 (2). We summarize both articles here due to their close relation. We identify the following legal criterion.

Legal Criterion 7.1 (tr)**.** *The VSP must record all essential actions of the online election. The VSP must protect the election protocol by means of qualified signatures according to the German Electronic Signature Act [102]. It must be possible to process the documentation by means of commercially available data processing systems. The election protocol comprises data, events and actions which are related to the operation of a particular election and which must be documented and stored securely according to legal provisions of electoral law holding in the particular case. In particular, the anonymous votes must be recorded in a way enabling reproduction of the tallying result at any time. Immediately after completion of the election, the accredited VSP must hand the election protocol over to the Election Host.*

The refinement is derived from the corresponding article §8 (5) of the VSP Act explanatory memorandum as well as from VSP Ordinance §4 (2). While the explanatory memorandum elaborates on the contents of the election protocol, the ordinance specifies protection measures. Recording an election protocol primarily enhances the verifiability of the election and therefore adds to the principle of trust.

Legal Requirement 8. *The VSP must ensure that after casting of votes no relationship between voter and voting decision can be established.*

This requirement represents VSP Act §8 (6). It can be refined as follows.

Legal Criterion 8.1 (se)**.** *The VSP must ensure that after casting of votes no relationship between voters and voting decision can be established. This requirement holds in particular for the storage of votes in the electronic ballot box, the tallying phase, as well as the secure storage due to the fulfillment of the obligation of documentation.*

The refinement is based on the associated information for VSP Act §8 (6) given in the corresponding article of the explanatory memorandum. Following the explanatory memorandum we match the requirement to the basic election principle *secrecy* (se). Next, we consider VSP Act §9.

Legal Requirement 9. *The VSP must advise the Election Host of the online election on the necessary measures to securely carry out the online election, and inform the Election Host about possible legal consequences if these measures are not implemented.*

This requirement represents VSP Act §9 (1). It can be refined as follows.

Legal Criterion 9.1 (–)**.** *The VSP must brief and advise the Election Host in an understandable manner at least on*

1. *the requirements satisfiable by its voting system and their suitability for carry out the ordered election,*
2. *the security and compatibility of the terminals and the communication system provided by the Election Host for performing the online election,*
3. *the security measures which have to be implemented by the Election Host (in particular, the VSP must inform the Election Host about the need for securing the terminal devices provided for the voters by means of protection software.),*
4. *the risks remaining after implementation of the security measures by the VSP and the Election Host,*
5. *possible legal consequences if these measures are not implemented,*
6. *the important functions of the online election,*
7. *the information which the Election Host needs in order to fulfill its control tasks.*

The additional information can be found in the corresponding article §9 (1) of the VSP Act explanatory memorandum as well as in the VSP Ordinance §5 (1). The security aspects addressed in this criterion are of a rather general nature. Hence we do not match it to specific election principles.

Legal Requirement 10. *The VSP must brief the voter on security measures the voter has to take. Therefore textual instructions are to be submitted to the voter. The voter must confirm particularly taking note of these instructions as a prerequisite for participating in the online election.*

This requirement from VSP Act §9 (2) is again concretized in the VSP Ordinance.

Legal Criterion 10.1 (–)**.** *The VSP must brief the voter in generally understandable language. To this end, the VSP must submit textual instructions in compliance with §126 German Civil Code [4] to the voter. The voter must confirm particularly taking note of these instructions as a prerequisite for participating in the online election. The instructions must comprise at least*

1. *the secure usage of securing means and appropriate measures after their loss,*
2. *the technical prerequisites for participation in the election,*
3. *the technical steps leading to casting of a vote,*
4. *the technical means available to the voter which can be used to detect and correct input errors before casting the vote,*
5. *the secure communication with the voting system of the VSP,*
6. *the necessary security precautions on the terminal used for the online election.*

The refinement is derived from VSP Ordinance §5 (2) as well as from article §9 (2) of the VSP Act explanatory memorandum. They specify in particular the content of the briefing. Like in the foregoing legal criterion, we do not match to specific election principles here. Next, we consider VSP Act §10.

Legal Requirement 11. *The VSP must document the measures taken to observe the VSP Act and the VSP Ordinance in a way, that the data and its integrity can be verified at any time.*

We identified the requirement in VSP Act §10 (1).

Legal Criterion 11.1 (–)**.** *The VSP must document at least all data proving fulfillment of the requirements for accreditation and observation of the safeguards according to the VSP Act and the VSP Ordinance in a way that the data and its integrity can be verified at any time, subsequent alteration must be detectable. The VSP shall store the documentation, in case it is no longer required for the accreditation of the VSP, for at least 30 additional years.*

This criterion is based on the additional information given in VSP Ordinance §4 (1) as well as the VSP Act explanatory memorandum for article §10 (1). Since it is not directly related to the security of the election procedure we do not match it to the basic election principles.

The last article under consideration is VSP Act §11. However, this article only addresses the regulation of the abandonment of practice of a VSP. It does not contain requirements that relate to the election procedure. Since we want to focus on requirements for a secure election procedure with VSPs we omit this article here. Now that we have considered all articles required according to VSP Act §4 (2) we address the remaining article §4 (3).

Legal Requirement/Criterion 12 (dp)**.** *The VSP must ensure that the design and the operation of its online voting services is in accordance with the legal provisions on data protection, especially the provisions of the German Federal and State Data Protection Acts and the German Teleservices Act [6, 10].*

This requirement has no refinements in the explanatory memorandum of the VSP Act or in the VSP Ordinance and is therefore considered a criterion as well.

4.4. Review

In this section we consider relevant issues regarding the application of the legal regulation for VSPs, its position with respect to a recent judgment of the German Constitutional Court regarding the use of electronic voting machines, and its applicability to political election scenarios.

4.4.1. Application and Implementation of the Legal Regulation

At the date of authoring this thesis, the legal regulation presented above is not yet in use. We briefly describe which steps have to be taken to apply and implement it[5]. Entities that want to implement their online elections with accredited VSPs may choose to employ them in various ways. Corporations may, for example, prescribe in its bylaws that if online elections are performed, accredited VSPs are to be assigned. Similarly, a public body may include the use of VSPs in its ordinances. The respective entity should then contact one of the accredited VSPs to enter in an online voting services contract.

For the presented approach to be implemented, the act has to pass the legislative procedure. Legislative competence lies with the German Bundestag, art. 74 I no. 11 of the German Basic Law [3]. A federal regulation is necessary pursuant to art. 72 II of the German Basic Law, since non-political elections often claim validity nationwide. Also, their similar performance nationwide asks for federal regulation.

4.4.2. Judgment of the German Constitutional Court

So far, electronic voting in Germany has only been regulated for federal parliamentary elections, and does not address remote voting, but merely electronic voting with machines at polling stations[5]. These have been increasingly used since 1999, especially for the election of the German Bundestag (Federal Diet). Their usage is regulated in the German Federal Electoral Act [7] and the German Federal Voting Machines Ordinance [18]. Subsequently, in early March 2009, the German Federal Constitutional Court rendered judgment on the use of voting machines in German parliamentary elections. This judgment has severe consequences for the development of electronic voting in Germany. In this section we therefore consider its relevance for the legal regulation for VSPs.

[5]This section can also be found in our publication [P3] with minor textual changes.

The decision had been precedented by the deployment and use of voting machines in the parliamentary elections for the German Bundestag in 2005. The court ruled act, ordinance and using the particular type of voting machine for political elections unconstitutional. It held that the technology that was used does not comply with the constitutional principle of "the public nature of elections" (see [57], [58]). This principle requires that voters be able to examine all essential steps of the voting and counting procedure in a reliable way without any specialist knowledge. Applied to electronic voting in general, the holding primarily makes the security objective of verifiability mandatory, including *individual verifiability* (every voter can verify that her vote was accounted for correctly) and *universal verifiability* (anyone is able to verify the correctness of the voting and tallying process) (cf. [93], [86] or [78]). Current online voting protocols use different approaches to provide verifiability. However, the verification functionality required by the judgment is not defined in detail. Moreover most protocols indeed require special knowledge of the voter in order to verify the election process. Consequently it is an open question to what extent current online voting protocols are able to observe the principle of the public nature of elections as required by the judgment. However, applying the reasoning of [38], the statements of the judgment do not prohibit online voting in non-political elections. The principle of the public nature of elections does not apply to all types of elections per se: The principle is not part of the expressly enumerated voting principles. The court derives it from German Constitutional Articles 38, 20.1 and 20.2 [3]. Its scope and limitations are therefore also developed by the judiciary. The present judgment as well as former judgments declared the principle as an integral part to a functioning democracy. Popular sovereignty demands that the public can effectively express its political opinion. This requires trust in the process by which its representatives are chosen. The voters need to be certain that their ballot carries its desired effect in transmitting their sovereignty to their representatives. It is thus necessary that the electoral process is performed "under the public eye" so that the sovereign may keep trust in his/her political participation. This however can only be assured by a right to immediate monitoring of the process. The counter-implication of the above is that the principle of the public nature of election does not have to be observed under all circumstances if an election does not transfer sovereignty from the public to the legislator. This is the case for most non-political elections [38].

Consequently, online voting systems may be implemented in accordance with the judgment in the following election scenarios: Non-political elections are not subject to the judgment's holding. As explained above, such elections generally do not need to observe the principle of the public nature of election. Hence, online voting here could be implemented as additional voting channel equal to the regular channel of voting at a polling station. However, in some non-political scenarios, other legal regulation specifically requires the principle of the public nature of elections. For example, elections of the works council in a company are required to observe this principle by the German Works Constitution Act [11]. Still, in such scenarios online voting may be implemented as an additional means of voting, where it can replace or support absentee voting. Here, the lack of voting transparency (public nature of elections) is legally acceptable: according to legal scholarship and prior decisions, the several election principles must

be balanced among each others. Limited compliance with one principle can be justified by benefits for others. Absentee voting benefits universal suffrage because it allows convenient access to the voting system from remote locations. Online voting can do the same by enabling the voter to vote from every place that has network access, including home or office. Therefore more people could exercise their right to vote, for example people who otherwise would not be able to go to a polling station. The legal regulation for VSPs in fact addresses online voting and restricts to non-political elections. It does not consider online voting as a replacement for voting at polling stations. Consequently the holding of the judgment on the public nature of elections does not apply to the scenarios considered in the legal regulation for VSPs.

4.4.3. Applicability of the Legal Regulation for VSPs to Political Elections

Following our previous reasoning, the requirements of the principle of the public nature of elections are not binding for the concept of a VSP in non-political elections. Now we address the question whether the legal regulation could be expanded such that the VSP concept could be used in parliamentary (i.e. political) elections[6]. Here, the principle of the public nature of elections would require the voting process and its result to be verifiable by the voter. Every voter must be able to perform the verification without any special knowledge. Satisfying both aspects at the same time is a technical challenge. Recent electronic voting protocols support different verifiability techniques like voter-verifiable receipts or a bulletin board (see for example the Helios scheme from Adida [27], the Prêt à Voter scheme from Ryan [45, 94], Neff's scheme [90], or the Scantegrity scheme from Chaum et al. [44]). Such protocols claim to provide end-to-end verifiability which minimizes the need to trust the correctness of the voting system by making the election procedure fully auditable (see also p. 2 and [81]). However, many of these protocols make heavy use of cryptography. In general, such schemes would probably be excluded by the law because they are not sufficiently understandable by the voters without specialist knowledge. The holding by the Constitutional Court would not permit this.

However a combination of technical and organizational approaches might be able to jointly satisfy what the principle of the public nature of elections requires. The court explicitly allowed for this option – as long as it leaves a means for individual verification of correct voting procedure (see [57, 58]). A solution could be based on an easy-to-understand voter-verifiable voting protocol. This should be implemented as open-source software, because the demand for verifiability of the system code would outweigh the business interest of the developer in keeping the code proprietary (see [51, 33]). The voting software should be embedded in a secure and trustworthy operational environment, which accredited VSPs could create. The voting software and the operational environment are to be evaluated and certified. Following the judgment, evaluation and certification procedures alone cannot replace personal verification by the voter. However we argue that as an additional component in a combined approach, such procedures

[6]Parts of this section can also be found in our publication [P3] with minor textual changes.

may indeed contribute to satisfying the requirements of the judgment (see also [51, 33]). Moreover, all essential steps of the voting process should be documented. The documentation must be publicly accessible for verification purposes as long as its disclosure does not violate the basic election principles or provisions regarding data protection. Assistance should be available to the voters at all time. Votes are to be stored outside the voting system for recount purposes by means of arbitrary counting software. These measures can be enforced by adjusting the legal regulation.

Addressing the requirement of 'verifiability without specialist knowledge' brings up the subject of usability (an introduction can be found in our publication [P6]). In the field of electronic voting, this has hardly been considered scientifically so far. Optimized voting protocols and self-explanatory graphical user interfaces might be necessary. We suppose that usability in electronic voting will have to be a major research topic as of now. The VSP can contribute here by providing competent and easily accessible assistance to the voters for help regarding the vote-casting process, and moreover by providing user-friendly designed ballots and verification mechanisms.

To sum up, expanding the application of the VSP to political election scenarios might be possible if the legal regulation is extended by strict provisions on verifiability and usability of the voting system. The implementation of these provisions will be difficult since optimized protocols may be required. But the presented combined approach of technical and organizational measures can reduce the problem significantly. As we have seen, this approach can be facilitated by implementing legally regulated VSPs. The final decision whether our proposal might satisfy the requirements of the judgment can only be answered by jurisdiction.

5. Security Concept Template

In this chapter we identify the technical requirements for Voting Service Providers (VSPs). To do so, we derive technical refinements from the previously identified legal criteria by applying the third step of the KORA methodology. For this purpose, we primarily use the technical requirements compiled by Volkamer [109] to adapt the legal criteria to the technical field of application. Thereby we derive enhanced technical requirements that comply with the legal regulation for VSPs. By integrating these technical requirements into the general structure for the Security Concept as given in the VSP Ordinance in Chapter 4.2 we obtain a template that precisely defines the required contents of the Security Concept of a VSP. Our template specifies all technical requirements for the voting system and the operational environment that a VSP has to satisfy in order to comply with the legal regulation. The Security Concept Template thereby supports a VSP in designing its facilities and processes adequately and provides a guideline how to create its Security Concept. Moreover, it facilitates the evaluation and certification of a VSP as it clearly defines what needs to be considered in the procedure. This makes the evaluation of VSPs more comparable and thereby helps to ensure a homogeneous security level among VSPs. The Security Concept Template represents the second building block of our security approach. This chapter is based on work we published in [P1] and [P5].

5.1. Overview of the Security Concept

First we summarize what needs to be included in the Security Concept. According to the legal regulation, the Security Concept serves as the basic proof of security of a VSP in the evaluation, certification and accreditation procedure. It demonstrates the VSP's compliance with the act and the ordinance. To this end the VSP specifies the safeguards that it implements in order to satisfy the legal provisions. The general contents of the Security Concept are set in the VSP Ordinance (see Chapter 4.2 and [92]). We distinguish two sections.

First, the VSP needs to specify the features and functions of its online voting service. For this purpose the VSP describes the technical, constructional and organizational safeguards and their suitability. This includes for example encrypted communication channels, physically secured server rooms, or a help desk for voter assistance. Moreover the VSP describes the technical products used for its online voting service. This includes the voting software and the hardware, for example the election server. The description of the technical products has to comprise product designation, manufacturer as well as statements concerning their legal conformity (cf. [92]).

Secondly, the VSP needs to demonstrate that the legal provisions are satisfied by suitable safeguards from the first section. According to the VSP Ordinance, the VSP has to describe the organization of setup and processes for its online voting service, its compliance with the election principles, with data protection acts, and with measures for ensuring and maintaining operation, especially in case of emergencies, as well as the procedures for evaluating and ensuring the reliability of the deployed personnel and at last, an estimation and validation of remaining security risks (cf. [92]). According to the explanatory memorandum of the VSP Ordinance (also given in [92]), this second section of the Security Concept refers to the articles §4 and §§ 7–10 of the VSP Act. All those are covered by the legal criteria that we derived from the VSP Act and the VSP Ordinance in the previous chapter. Hence these criteria are what the VSP needs to consider. However in its Security Concept the VSP is supposed to demonstrate how they are technically satisfied. This requires a technical interpretation of the legal criteria. We provide this in the next section.

5.2. Technical Security Requirements

The legal criteria for VSPs need to be technically interpretable in order to ensure their correct technical implementation by corresponding safeguards. This is a prerequisite for the secure construction of VSPs as well as the evaluation and certification of their compliance with the VSP Act and the VSP Ordinance. Therefore we derive corresponding technical requirements. To do so, we implement the third step of the KORA methodology. We use additional sources to technically refine the legal criteria we identified in Chapter 4.3. The first source is the technical documentation of requirements for remote electronic voting from Volkamer's PhD thesis "Evaluation of Electronic Voting – Requirements and Evaluation Procedures to Support Responsible Election Authorities" [109, Chapter 6]. This most recent collection is based on a comprehensive analysis of current literature on requirements for electronic voting (see [109, p. 35]), including for example the approved recommendations on "Legal, Operational and Technical Standards for E-voting" of the Council of Europe [48], the requirements catalog "Online-Voting Systems for Non-parliamentary Elections" developed by the German National Metrology Institute[1] [75] as well as the German federal regulations for electronic voting machines [18]. We identify the suitable requirements from Volkamer based on their classification regarding the affected election principles. All technical requirements we used from Volkamer are listed in the appendix in Chapter A.3 for further reference. As far as possible we take the exact wording of Volkamer to ensure the correctness of the requirements. Only where necessary we adjust Volkamer's formulation to the specifics of the VSP context, for example by replacing subjects or objects with the corresponding counterparts. The second source for refinements is the explanatory memorandum of the VSP Ordinance [92]. In the previous chapter the VSP Ordinance served as the basis for the legal criteria. The explanatory memorandum now contains additional details on the particular articles of the ordinance with regard to their legal or technical background

[1] In German: Physikalisch-Technische Bundesanstalt, PTB

as well as their intended interpretation and implementation. As in Chapter 4.3, we translate the relevant passages of the explanatory memorandum into English since the original text is in German.

Regarding the wording in the technical requirements within this section, we follow the recommendations of the RFC 2119: "The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119" (cf. [36]).

We start with Legal Criterion 1.1. It considers the reliability of the VSP's personnel. We formulate the following technical refinement.

Technical Requirement 1. *The VSP must ensure the reliability of its deployed personnel at any time, not only during operation. The reliability must be proven by means of up to date certificate of good conduct according to the Federal Central Criminal Register Act §30 (5) [5]. The VSP must ensure the specialist qualification of its deployed personnel necessary for particular tasks during operation by means of respective certificates which prove that the qualification for the particular job specification is sufficient. The VSP shall educate its deployed personnel in the use of the online voting system and shall ensure that information provided to them is understandable.*

Due to its general nature, Legal Criterion 1.1 has been classified (all) in Chapter 4.3. That means it might affect all election principles. The technical requirements in Volkamer's thesis are also classified according to the election principles they support. So we examined all requirements with the same corresponding classification in order to find those that provide suitable technical details to refine the Legal Criterion at hand. Among them we identified Op.6 to suit the context. It specifies how to educate the poll workers (see Appendix A.3 for the full text). We adapted Op.6 to the VSP scenario by matching the corresponding roles (e.g. the poll workers are the VSP's personnel). Next we considered the second source of refinements: the explanatory memorandum of the VSP Ordinance. Legal Criterion 1.1 is based on VSP Ordinance §1. For this article, the explanatory memorandum adds details on the time frame for which the reliability of the personnel is required. This concludes the refinement.

The next Legal Criterion 1.2 deals with the VSP's obligation to estimate residual security risks of the online voting service in order to evaluate its reliability.

Technical Requirement 2. *The VSP must provide an estimation and validation of remaining security risks. This relates to the residual risk of system failure or interruption in particular with regard to deployed technology. The VSP may refer to valuation from evaluation authorities or manufacturers of deployed products or technology.*

This topic is not considered in Volkamer's set of requirements. However we added information from the related article §1 of the explanatory memorandum of the VSP Ordinance. It specifies the intended emergency situation and proposes how the residual risk can be valuated.

Coming up next, we refine the Legal Criterion on the availability of the VSP's voting service.

Technical Requirement 3. *The VSP must ensure by means of suitable measures that the communication and voting system is available during at least 95% of the election period and that it enables counting of votes after the end of the voting process. Therefore the VSP shall implement suitable safeguards like backup systems or redundant components.*

The underlying Legal Criterion 2.1 is classified (un) because availability is a precondition for the basic principle of an universal election. Volkamer defines several (un)-requirements of which we identified O.OSP.Availability to suit the context in the present case. It states that the voting system "should be available during the whole polling phase". Still we kept the formulation "available during at least 95% of the election period" because the intention is to refine but not to change the legal demands. That does not interfere with Volkamer's definition because it uses the wording "should". This allows for a variance in case of valid reasons which the legal demand represents in this case (see the RFC definition in [36] and also Volkamer [109, p. 64]). Finally we examined the corresponding article §3 (1) of the explanatory memorandum of the VSP Ordinance for further details. It proposes technical safeguards for a high-availability system that we added to this technical requirement.

Next we consider how the VSP has to handle occurring interruptions of its online voting service.

Technical Requirement 4. *Upon exceptions, malfunctions, and breakdowns the online voting system must ensure a secure restart sustaining the legal election principles, no voter must lose his right to cast a vote nor get the possibility to cast two votes. To this end, the online voting system shall be capable to determine whether a particular voter cast a vote and his electronic vote was successfully stored in case of exceptions, malfunctions, and breakdowns. The voting server shall run a self-check before resuming is possible. In case of irreversible problems the voting server shall prevent resuming of the voting phase. During system interruptions, malfunctions and breakdowns, the online voting system shall prevent loss of data including the votes already cast and all necessary data present before interruption. The VSP must inform the Election Host about these interruptions and perform tests in his presence in order to demonstrate the secure condition of the communication and the voting system and the secure restart.*

Here we refined Legal Criterion 2.2 which is labeled (un, di). Among the requirements for a universal or direct election, Volkamer provides three that match the present context: O.OSP.VoteRightExc, O.OSP.ErrorRecovery and O.OSP.DataLoss. They add details on preserving voting privileges during specific types of interruptions, and explain how to securely resume afterwards without losing election data. Regarding the VSP Ordinance explanatory memorandum, we included the specifics given in article §3 (1) on the necessary interaction between VSP and Election Host during system interruptions.

The next technical requirement refines Legal Criterion 2.3 that takes into account the guarantee and maintenance of operation of the online voting service, even in case of emergencies.

Technical Requirement 5. *The VSP shall implement precautions to guarantee and maintain the operation of the online voting service. That includes at least a 24h emergency service at least during the voting phase, safeguards against power failure, voltage fluctuation, environmental effects (for instance, mechanical, electromagnetic, and climatic) to the voting server, unexpected user activity, fire, water, network problems or comparable incidents. The VSP shall develop a contingency plan describing appropriate responses to at least the following circumstances:*

- *results produced by recount or alternative tallying software do not agree with original result,*
- *number of votes recorded does not match number of electors,*
- *any kind of exceptions, malfunctions, and breakdowns.*

Legal Criterion 2.3 is labeled (un, tr) meaning it supports the principle of an universal election and the principle of trust. Examining the corresponding requirements from Volkamer, we identified Op.1 as well as O.OSP.Availability to deal with emergency precautions. We used the information given in the application note of O.OSP.Availability to further specify potential emergency situations. Moreover we included the requirement for contingency planning from Op.1. Then we considered the corresponding article §1 of the VSP Ordinance explanatory memorandum and added the specific descriptions of the emergencies as well as the requirement for a 24h service.

Now we refine the legal demands for confidentiality of the online election introduced in Legal Criterion 2.4.

Technical Requirement 6. *The online voting system must transmit, receive and store identification and authentication data of the voters and electronic votes protected from unauthorized disclosure. Therefore the VSP shall ensure the confidentiality of all data communication by means of technical safeguards like secure channels and organizational precautions like a system to manage access privileges. On the voting server, the VSP shall implement an access control policy for the VSP personnel interface which restricts all activities to particular user roles and requires physical presence. The access control mechanism shall only allow access to the voting server if at least two different users are logged on.*

By following the classification (un, fr) for the principles of a universal and free election we identified O.T.SecretAuthNet, O.T.IntResultNet, O.T.AC, and O.OSP.SepDuty to be suitable for refining this legal criterion. The first two deal with the confidential transmission of authentication data and electronic votes. Thereby they consider the aspect of unauthorized network access and mainly coincide with the legal criterion. The latter two however provide specifics on the protection of stored data against unauthorized access and introduce the concept of the separation of duties. Thereby they extend the demand for protection against unauthorized disclosure with respect to the threat of unauthorized physical access. At last, we added possible technical measures to ensure confidential communication that are mentioned in the VSP Ordinance explanatory memorandum §3 (1).

The next item concerns the secure authentication of the voters which is of great importance to ensure the principle of an equal election.

Technical Requirement 7. *The VSP shall unambiguously identify and authenticate the voter before storing his vote in the electronic ballot box. The VSP must accomplish identification and authentication of the voter by use of at least two independent securing means. At present, PIN/TAN, smart cards for digital signatures or the application of biometry are considered reliable securing means. The VSP must ensure that upon correct usage of the securing means, casting of a vote by individuals not eligible to vote or casting of multiple votes by individuals entitled to vote is prevented. The VSP must ensure confidential and unaltered handover of the securing means for identification and authentication to the voter's power of disposition and develop secure procedures for storage and management of the identification and authentication means where necessary. The client-side voting software shall only communicate with the authentic and unaltered voting server. The voting server shall communicate only with the authentic and unaltered client-side voting software.*

Here we concretize Legal Criterion 2.5 which is labeled (eq, un, di). From the corresponding requirements from Volkamer we integrated O.T.IneligVoter, Op.7, O.T.WrongSW, and O.T.WrongServer. They complement the basic requirement for authentication of the voters by taking into account the secure handover of the necessary authentication credentials as well as the authentic communication of voter and voting system. Some of those requirements from Volkamer are labeled (all) which means they add to all election principles. Since they perfectly match the context of the legal criterion at hand we included them in the refinement. Regarding the VSP Ordinance explanatory memorandum, we added details from article §3 (3) that lists exemplary technical measures for secure authentication.

Another major requirement for secure online elections is the integrity of voting documents considered in Legal Criterion 2.6.

Technical Requirement 8. *The voting system must be able to detect unauthorized modification, erasure and addition of identification data of the voters, votes, protocol data and further relevant data. Alteration of election data must be recognizable at any time, the VSP shall verify the freshness, authenticity, integrity, and format correctness of all messages before processing them. The VSP shall ensure the integrity of all data communication by means of technical safeguards like secure channels and organizational precautions like a system to manage access privileges. The VSP shall prevent data loss during normal operations and in case of exceptions, malfunctions, and breakdowns.*

Following the label (di, un, tr) of Legal Criterion 2.6 we included O.T.AlterMsgNet, O.T.IntegVotes, O.T.IntegElecData, O.T.DeleteMsgNet and O.OSP.DataLoss from Volkamer based on their allocation to the principles of trust and a direct and universal election. They contain refinements regarding the protection of the integrity of votes and election data and during the general processing of all messages. Moreover they add the

aspect of protecting the integrity of system components. The VSP Ordinance explanatory memorandum §3 (3) again provides exemplary protective measures to further refine the legal criterion.

The following requirements are mostly concerned with the voting operation. First the voting system has to be set up correctly.

Technical Requirement 9. *The VSP must take over the registers of persons entitled to vote and persons with the right to stand for election from the Election Host for use in the online voting service. The lists are transmitted in written or electronic form, the VSP must transfer them into the voting system correctly and reliably. Therefore the VSP shall develop procedures to configure the voting server (including ballot details, order on voting server, and tallying software).*

Here we refine Legal Criterion 3.1. It is labeled (di) as it affects the principle of a direct election. The requirement is very specific, so there are no appropriate (di)-requirements in Volkamer's list. However, among the (all)-requirements we identified Op.7 to suit the context. We did not add Op.7 completely because it covers a number of aspects that are considered in other technical requirements. Still we included the given specifics on the secure configuration of the voting server.

The next requirement is a refinement of Legal Criterion 4.1. It ensures that the Election Host retains control over specific functions in order to observe his legal obligations.

Technical Requirement 10. *The VSP must provide a remote interface to the Election Host with the following functionality:*

- *identification and authentication,*
- *starting the voting phase which is only possible once,*
- *resuming the voting phase after any kind of exceptions, malfunctions, and breakdowns,*
- *closing the voting phase after which the actions 'starting' and 'resuming' are disabled,*
- *starting the tallying phase only after having closed the voting phase.*

Legal Criterion 4.1 is not classified to support specific election principles. Nevertheless we identified O.OSP.PWInterface in Volkamer's list to match the context. Originally it is labeled (se, fr) because its intention is to limit the system information presented to the poll workers. But for the context at hand it provides a technical specification of the legal demands. Therefore we slightly adjusted Volkamer's wording to the VSP scenario and included the parts that match Legal Criterion 4.1. Following the related article §3 (2) of the explanatory memorandum of theVSP Ordinance, we added the detail of making the control functions available to the Election Host via remote access. This is of course due to the fact that the VSP carries out elections as a remote service.

Now the initial state of the voting system is to be checked. We refine Legal Criterion 4.2.

Technical Requirement 11. *Directly before starting the voting procedure, the VSP must enable the Election Host to verify that the ballot box does not contain any votes and that all other parts of the voting system, for example the electoral roll, are in their predefined initial state. Therefore the voting server shall provide the functionality to completely delete all data from previous elections. Moreover the VSP shall develop procedures to check the voting server (including configuration and empty ballot box) as well as to ensure that the voting server is in the appropriate state at every stage in the election phase. The voting server shall be capable of performing self-checks. It should regularly perform automatic self-checks and report the results to the VSP's personnel. At last the VSP must provide an interface to the Election Host with the following functionality:*

- *checking that the voting server has been set up correctly (for example, order of voting options and empty electronic ballot box),*
- *performing self-checks,*
- *checking the current state.*

Legal Criterion 4.2 is classified to support the principal of a direct election. In Volkamer's list, we identified the corresponding requirements O.OSP.SelfCheck, O.OSP.-DeleteData, and Op.7 to fit into this context. They specify self-checking procedures for the voting system. Again we added suitable parts of O.OSP.PWInterface. Just like in the foregoing Technical Requirement 11 we cannot associate this (se, fr)-requirement based on the supported election principles. Still it is particularly suitable to provide a technical specification for the requirement at hand. Therefore we adapted the requirement to the VSP scenario: the "poll worker interface" is changed to the "Election Host interface" and the range of functions is reduced to what is necessary in this technical requirement. Finally, we examined the corresponding article §3 (2) of the explanatory memorandum of the VSP Ordinance. It adds information on the importance of checking the electoral roll during set up.

The next technical requirement refines Legal Criterion 4.3. It considers the closure of the voting phase.

Technical Requirement 12. *After closing of the voting, the VSP must allow voting procedures already in progress, like the correction of the electronic ballot or its final submission, to be completed within the time limit set before starting the election by the Election Host. The acceptance of electronic votes into the electronic ballot box should remain open for a sufficient phase of time to allow for any delay of data transport. However logging on to the voting system must not be possible any longer. After expiration of the time limit, further voting procedures, voting related transmissions, acceptance of further votes and restarting of the online voting system must not be possible, only tallying must be allowed. The VSP must provide an interface for the Election Host that warns the Election Host if he tries to close the election before the final date.*

The underlying Legal Criterion 4.3 is labeled to support the principle of an universal election. Among the corresponding requirements from Volkamer O.OSP.ClosePoll and

O.OSP.PWClosePoll provide suitable details to concretize the legal criterion. The first one introduces the aspect of a network delay that has to be considered when closing the voting phase. The latter one provides specifics on how to inform the Election Host about the status of the closing procedure using an interface. We adapted the roles to the appropriate counterparts in the VSP scenario and finally included the identified additions. The explanatory memorandum for article §3 (2) of the VSP Ordinance adds details regarding the questions which voting procedures are allowed to be extended beyond the time limit and what is to be done after shutting down the voting phase.

Now we concretize Legal Criterion 5.1 which concerns the representation of the electronic ballot.

Technical Requirement 13. *The VSP shall accurately display the authentic and unaltered electronic ballot. Therefore it must display the whole content of the electronic ballot in a reasonable discernible manner without excessive scrolling or zooming. Furthermore the VSP must grant the same space for each voting option and implement the representation options as requested by the Election Host corresponding to election specific legal provisions. If polling booth voting or absentee voting is available as alternative voting channel, the representation of both the electronic ballot and the paper ballot must be equivalent. If only a snippet of the whole electronic ballot is visible, the VSP must make the voter aware of that circumstance. The VSP should ensure that all online voting system display the ballot in a uniform way. Therefore the client-side voting software shall ensure equality and accuracy of presentation of the voting options on any vote-casting device. The online voting system shall avoid the display of other influencing messages.*

Legal Criterion 5.1 is classified (fr) as it supports the principle of a free election. Therefore we examined all (fr)-requirements from Volkamer's list and incorporated O.OSP.-AccurDisp, O.OSP.EqualPres, and Op.13. We added the given details regarding the representation of the ballot on different voting devices. The VSP Ordinance's explanatory memorandum for article §3 (4) specifies the term "reasonable discernible". In particular we included the supplements concerning accurate display like prevention of scrolling and zooming, as well as the equivalent representation for different voting channels.

The specific legal demands for the ballot casting procedure are concretized in the next technical requirement.

Technical Requirement 14. *The VSP shall ensure that the voters*

1. *are able to identify and authenticate themselves,*
2. *are able to make and to cast a voting decision,*
3. *are able to spoil their vote, i.e. to cast an invalid vote (The client-side voting software should warn the voters when they try to spoil their votes in one or more polls.),*
4. *are able to abort the voting procedure at any time without loosing elective franchise,*
5. *are able to correct their vote any number of times until the final voting,*

6. *receive a confirmation regarding the status of their vote – at least the information that their electronic votes have been successfully stored (In case the voter does not receive the confirmation, he shall get this information as soon as he logs on again.),*

7. *are not enabled by the voting system show their voting decision to others. In particular, the voters must not be able to construct a receipt proving their vote. Neither information sent to, displayed on, sent from, nor intermediate results calculated on their vote-casting device or protocol messages sequences shall serve as proof. To this end, the VSP shall not provide any information in the transmitted protocol messages, which allows to construct the link between a particular voter and his vote. The VSP shall ensure that neither the vote itself nor the number of chosen voting options (including an empty ballot), nor a spoilt vote (for example, by using the length of the protocol messages) can be linked to a particular voter. In addition, it shall be ensured that the sequence of messages does not reveal the link.*

8. *The VSP shall coordinate different voting channels, for instance, it shall prevent voters casting one vote per possible channel and shall develop a procedure to merge the results from different channels.*

This technical requirement is based on Legal Criterion 5.2 which classifies the single parts differently. Therefore we searched Volkamer's list to identify suitable technical specifications for each part separately. Each of them matches the election principles reflected in the respective part of the legal criterion. In order of appearance we used O.OSP.Interface, O.OSP.Spoil, O.OSP.SpoilWarning, O.OSP.Confirmation, O.T.ProofGen, O.T.ElecSecrecyNet, and Op.5 for the refinement. The first one extends the list at the beginning by adding the requirement for identification and authentication of the voters prior to casting a ballot. The next two provide details on the ability to cast invalid votes. Then O.OSP.Confirmation specifies the message confirming the voting process. O.T.ProofGen and O.T.ElecSecrecyNet provide comprehensive details how to prevent constructing a proof for voting. At last, Op.5 adds a new item to the list regarding the handling of additional voting channels. Regarding the ballot casting procedure, there are no additional information available in the explanatory memorandum of the VSP Ordinance.

The next technical requirement refines the security aspects of the tallying procedure.

Technical Requirement 15. *The VSP shall ensure that the tallying software accurately calculates results using the appropriate algorithm based on all (authorized) electronic votes stored in the electronic ballot box and only based on these electronic votes, and that the single steps can be verified and reproduced at any time afterwards. Furthermore the VSP shall ensure the integrity and completeness of the votes intended for tallying by means which allow for their verification. The tallying software shall verify the integrity and authenticity of the electronic votes and protect the integrity and authenticity of election data as soon as the tallying is completed. The tallying software shall ensure that its operations and data are unaffected by other applications. The VSP should arrange alternative tallying software to check results. The online voting system shall provide the*

functionality to upload electronic votes into any tallying software. The counting of votes must be initiated publicly in the premises of the Election Host and the result must be published.

The underlying Legal Criterion 6.1 is classified to affect the principles of trust and a direct election. Among the corresponding requirements from Volkamer we identify O.T.-AuthCheckCount, O.T.IntegElecData, O.T.AffectCounting, O.OSP.AccurCalc, Op.11, and O.OSP.ReadToOtherSystems to suit the context at hand. They are mostly concerned with the integrity and verifiability of the tallying procedure and the protection of the related election data. In particular, Op.11 and O.OSP.ReadToOtherSystems add details to verify and reproduce the tallying result by making the data readable by alternative software. The explanatory memorandum of the VSP Ordinance does not provide any supplements for the legal criterion.

Next, we refine the VSP's obligation to record relevant election data during the election. The technical requirement regards the general obligation, the content of the election protocol and its protection.

Technical Requirement 16. *The VSP must record all essential actions of the online election. The voting server shall be capable of producing comprehensive audit data. The audit system shall provide the functionality to record, monitor, and verify audit data. Therefore the audit system shall have access to a reliable time source. Immediately after completion of the election, the VSP must hand the election protocol over to the Election Host. The VSP shall record the following:*

1. *all data, events and actions which are related to the operation of a particular election and which must be documented and stored securely according to legal provisions of electoral law holding in the particular case,*

2. *the anonymous votes must be recorded in a way enabling reproduction of the tallying result at any time,*

3. *the system configuration (including software version numbers) and election configuration (including voting option information) on the voting server at least at the beginning and the end of the polling phase, as well as before and after tallying,*

4. *a timestamp, the nature of the action, and the ID of the particular poll worker (where available) for every action performed by VSP personnel,*

5. *breakdowns, exceptions, malfunctions, and results of any self-checks (with timestamps, where appropriate).*

The VSP shall protect the integrity and authenticity of the election protocol including logs, other protocol data and electronic votes. It must be protected by means of qualified signatures according to the German Electronic Signature Act [102]. The audit system shall check the electronic ballot box, the ballot content, and the authentication data for evidence of tampering. Moreover the audit system and its records should be tamper-resistant and shall be tamper-evident. It must be possible to process the documentation by

means of commercially available data processing systems to allow archiving the electronic data outside of the voting system of the VSP without losing readability and verifiability of the tallying process. Especially the electronic votes must be stored in a way enabling recounting by means of arbitrary tallying software. The audit system should not record any information which might endanger the secrecy of the vote. Where such information is stored it shall only be accessible to those with appropriate authority. Therefore the audit system shall implement an adequate access control policy.

The underlying Legal Criterion 7.1 is classified (tr) since the election protocol improves the trustworthiness of the election procedure. Among the correspondingly labeled requirements from Volkamer there is a large set explicitly pointing at the election auditing. In particular we used the following requirements to concretize the legal demands. O.OSP.Auditing, O.OSP.Audit1, and O.OSP.Audit3 describe the general auditing procedure and add technical specifics like the necessary time source. O.OSP.Audit4, O.OSP.-Audit7, and O.OSP.Audit8 provide details on the content of the election protocol. They include the system configuration, the ID of involved poll workers as well as breakdown events in the protocol. Finally, O.OSP.Audit2, O.OSP.Audit5, O.OSP.Audit6, O.OSP.-Audit9, and O.OSP.Audit10 specify the protection of the recorded protocol data. In particular they require protection against tampering with the data or the system to protect the integrity and authenticity of the protocol. Moreover they ensure that the protocol data do not break election secrecy and therefore require an access control policy. Like before, we adapted these requirements to the VSP scenario by matching subjects and objects to their respective counterparts. We point out that O.OSP.Audit11 admittedly is related to auditing but is allocated to the principle of data protection and therefore used in the corresponding Technical Requirement 21 below. In addition, the corresponding article §4 (2) of the explanatory memorandum of the VSP Ordinance specifies the protection of the election protocol using qualified electronic signatures. Moreover it adds the requirement for maintaining the readability of the protocol even when it is archived outside of the VSP's system.

In the next technical requirement we concretize Legal Criterion 8.1 that concerns the anonymity of voters during the election.

Technical Requirement 17. *The VSP must ensure that after casting of votes no relationship between voters and voting decision can be established. This requirement holds in particular for the storage of votes in the electronic ballot box, the tallying phase, as well as the secure storage due to the fulfillment of the obligation of documentation. The voting server should not store any information which could link the voter with his vote after the completion of the voting process. Where any information which could link the voter to his vote is stored on the voting server, it shall only be accessible to those with appropriate authority[2]. In case of exceptions, malfunctions, and breakdowns, the voting server shall not reveal the link from the last voter to his selections or vote. The*

[2] According to Volkamer, no such authorities exist in most constituencies. Generally, access to such information might be required by or granted to certain user roles depending on the functionality of the voting software (e.g. for verification purposes) (see [109, p. 61]).

online voting system shall delete any records related to the voter's voting process from the vote-casting device when finishing the voting process.

The underlying Legal Criterion 8.1 is classified to support the election principal of secrecy (se). Volkamer lists the (se)-requirements O.T.ElectionSecrecy, O.OSP.Secrecy-AfterBreakd, and O.T.DeleteRecord. They specify storage and accessibility of data in order to maintain election secrecy even after system malfunctions and also consider the deletion of data on the voting device. We added those requirements, no adaptation to the VSP context was necessary. O.T.ProofGen is another (se)-requirement. However it is more related to Technical Requirement 14 and thus included there. There are no further refinements in the VSP Ordinance explanatory memorandum available to be used here.

Next, the legal regulation requires the VSP to brief and advise the Election Host as well as the voter. First we refine the Election Host briefing that is defined in Legal Criterion 9.1.

Technical Requirement 18. *The VSP must brief and advise the Election Host in an understandable manner on*

1. *the requirements satisfiable by its voting system and their suitability for carry out the ordered election,*
2. *the security and compatibility of the terminal devices and the communication system provided by the Election Host for performing the online election,*
3. *the security measures which have to be implemented by the Election Host (In particular, the VSP must inform the Election Host about the need for securing the terminal devices provided for the voters by means of protection software.),*
4. *the risks remaining after implementation of the security measures by the VSP and the Election Host,*
5. *possible legal consequences if these measures are not implemented,*
6. *the important functions of the online election, and*
7. *the information which the Election Host needs in order to fulfill its control tasks.*

Legal Criterion 9.1 is specific for the VSP scenario and not directly related to the general election principles. We therefore analyzed the technical documentation from Volkamer in terms of content. However there is no technical requirement that fits the context. The same holds for the explanatory memorandum of the VSP Ordinance. The corresponding article §5 (1) does not provide further details. We therefore leave the legal criterion unchanged.

For the briefing of the voter, however, we present the following refinement of Legal Criterion 10.1.

Technical Requirement 19. *The VSP must brief the voter in generally understandable language on security measures the voter has to take. To this end, the VSP must submit textual instructions in compliance with §126 German Civil Code [4] to the voter. The voter must confirm particularly taking note of these instructions as a prerequisite for participating in the online election. This requirement can be satisfied electronically if after successful logging on to the online voting system the voter must confirm knowledge of the instructions in order to get access to the next steps of the online election. The VSP shall brief and advise the voter at least on*

1. *the secure usage of securing means and appropriate measures after their loss,*
2. *the technical prerequisites for participation in the election,*
3. *the technical steps leading to casting of a vote,*
4. *the technical means available to the voter which can be used to detect and correct input errors before casting the vote,*
5. *the secure communication with the voting system of the VSP,*
6. *the necessary security precautions on the terminal device used for the online election.*

Beyond voter instruction, the VSP should provide a help desk service for the voters. This service should be based on a contractual agreement with the Election Host.

Legal Criterion 10.1 does not affect specific election principles either. We indeed identified Op.9 in Volkamers list to suit the context but it does not provide further technical details. In contrast, the explanatory memorandum for article §5 (2) of the VSP Ordinance adds information on how the required confirmation of the voter could be implemented. Moreover the help desk is introduced concretizing the way of briefing the voters.

Next, we regard Legal Criterion 11.1 which obligates the VSP to document its adherence to the law.

Technical Requirement 20. *The VSP must document at least all data proving fulfillment of the requirements for accreditation and observation of the safeguards according to the VSP Act and the VSP Ordinance. This concerns events and actions of the operation of an accredited VSP that are not directly related to the accreditation procedure and not documented anyway. The VSP must ensure that the documentation data and its integrity can be verified at any time, subsequent alteration must be detectable. The VSP shall store the documentation, in case it is no longer required for the accreditation of the VSP, for at least 30 additional years.*

Again, due to the specific nature of this legal criterion there is no suitable requirement in Volkamer's list that could be used as a refinement. In contrast, §4 (1) of the explanatory memorandum of the VSP Ordinance further concretizes the contents of this documentation.

Finally we present the technical requirement for data protection.

Technical Requirement 21. *The VSP must ensure that the operation of its online voting services is in accordance with the legal provisions on data protection, especially the provisions of the German Federal Data Protection Act [6], the German State Data Protection Acts and the German Teleservices Act [10]. This holds in particular for the audit system and for transmission of personal data by the online voting system. The implementation of data protection must be proven in a corresponding data protection concept unless the VSP already has a data protection audit certificate.*

Here Legal Criterion 12 is concretized using the (dp)-requirements O.T.PersonalData-Net and O.OSP.Audit11 from Volkamer. They provide specifics regarding the data that has to be protected and moreover require in particular the audit system to ensure data protection. The explanatory memorandum of the VSP Ordinance provides further information how the implementation of data protection is to be proven by means of a data protection audit certificate.

6. Evaluation, Certification and Accreditation

The goal of this chapter is to derive a concept to verify the security of online elections with a Voting Service Provider (VSP). To this end, we demonstrate the suitability of the evaluation and certification methodologies we proposed in Chapter 3. We apply the Common Criteria Protection Profile for online voting products [64] and the IT-Grundschutz catalog [59] to the technical requirements of the Security Concept Template. Thereby our overall approach makes the security of both the voting software and the operational environment verifiable and confirms the VSP's compliance with the legal regulation. The legally based procedure enables accredited VSPs to implement even legally binding online elections. Finally we provide recommendations for the appropriate usage of the proposed methodologies in the VSP context. Then we examine the legal accreditation procedure for VSPs and discuss some related issues. The evaluation, certification and accreditation concept represents the third building block of our security approach. This chapter is based on work we published in [P1], [P2], [P3], and [P5].

6.1. Applying Common Criteria and IT-Grundschutz

For the evaluation and certification of VSPs we introduced the methodologies Common Criteria and IT-Grundschutz in Chapter 3. Now we apply them to the technical requirements for VSPs that we identified in Chapter 5.2. Here Common Criteria deals with the security of the voting software while IT-Grundschutz targets the security of the operational environment. We analyze whether the technical requirements can be satisfied by a voting software certified according to the Common Criteria Protection Profile for online voting products and an operational environment certified according to IT-Grundschutz.

We shortly describe our approach. The Protection Profile is the basic document in the Common Criteria procedure. Briefly it specifies security objectives for a generalized product class, for example for electronic identity cards or biometric verification mechanisms (see [60, 68] for examples). A certified product is then proven to achieve these security objectives. A detailed introduction to Common Criteria and Protection Profiles can be found in [23]. For our analysis we use the "Common Criteria Protection Profile for Basic set of security requirements for Online Voting Products" (see [64]). It specifies the basic security objectives for online voting software. We analyze to what extent these security objectives are able to satisfy those technical requirements for the VSP that concern the voting software. For the technical requirements that concern the operational environment we use the safeguards of the IT-Grundschutz catalog [59] instead. These

predefined safeguards are specified to satisfy the typical security requirements of technical and organizational components of a general IT infrastructure. In IT-Grundschutz these components are called modules. They comprise generic aspects (e.g. personnel, contingency planning), infrastructure (e.g. server room), IT systems (e.g. server), network components (e.g. gateways) and applications (e.g. database). Each module is associated with specific safeguards that ensure its security. They can be adapted to the specific scenario to ensure appropriate function. A detailed introduction to the IT-Grundschutz procedure can be found in [61] and [62]. The modules and safeguards are described in [59].

We proceed as follows. For each technical requirement from Chapter 5.2 we first state the result of our analysis: *completely*, *partially*, or *not* satisfied by Common Criteria and/or IT-Grundschutz. Then we present the reasoning that lead to the statement. To this end we identify applicable security objectives (denoted by O.xxx as in [64, Chapter 4.1]) of the Protection Profile (PP)[1] for online voting products and/or IT-Grundschutz modules and safeguards (denoted by B x.xx and S x.xx as in [59]) respectively. Regarding the voting software we determine the suitability of the security objectives by comparing their properties as described in [64] with the technical requirements. Regarding the operational environment we base our analysis on the generic VSP architecture we described in Chapter 2. For each technical requirement we map the relevant components of the VSP architecture to suitable IT-Grundschutz modules from the catalog [59]. Then we examine the associated IT-Grundschutz safeguards and identify those that are suitable to satisfy the technical requirement.

Technical Requirement 1 *can be partially satisfied by IT-Grundschutz.*

The personnel is part of the VSP's operational environment. Therefore we apply IT-Grundschutz here. In an IT-Grundschutz evaluation and certification the modules of the family B 1.x "Generic aspects of IT security" must always be applied [59, p. 27]. This includes module "B 1.2 Personnel". Technical Requirement 1 first considers the reliability of personnel. Here the module B 1.2 contains the following suitable safeguards that we include: S 3.50 to select the personnel, S 3.2 to ensure commitment of staff members to compliance with relevant laws, regulations and provisions, and S 3.10 to select a trustworthy administrator. Moreover the safeguards ensure a security vetting of personnel (S 3.33) and the signing of non-disclosure agreements (M 3.55)[2]. However, IT-Grundschutz does not explicitly require the personnel to present a certificate of good conduct according to Federal Central Criminal Register Act as prescribed by Technical Requirement 1. Hence the VSP must require its personnel to present such certificates in addition to the IT-Grundschutz safeguards.

Next Technical Requirement 1 requires the personnel to have a specialist qualification. IT-Grundschutz provides a list of suitable safeguards concerning the training of person-

[1] From this point on, "PP" refers to the Protection Profile for online voting products [64].

[2] This safeguard is currently only included in the latest German release of the IT-Grundschutz catalog [65], therefore S is replaced by M.

nel regarding expertise and security awareness. The aforementioned module B 1.2 and the module B 1.13 for "IT Security awareness and training" implement corresponding safeguards. We include the most suitable ones as follows. S 3.51 defines the parameters for an appropriate concept for deployment and training of personnel. S 3.4 ensures training of the personnel regarding specialist knowledge required to use a specific application. S 3.5 provides a concept in order to train personnel on IT security related risks and appropriate behavior with regard to general and application specific aspects. S 3.11 ensures special training of personnel for administration and maintenance. S 3.45 defines the level of IT security related education for different types of staff members like superiors, IT security management, persons in charge of infrastructure, or administrators. While these safeguards cover most aspects of the necessary specialist education for VSP's personnel, they need to be adapted to fulfill the specific requirements of the legal regulation for VSPs. Staff members that operate critical functions of the voting system need very specific training. Moreover IT-Grundschutz does not strictly require the personnel to provide a proof of knowledge. The VSP therefore must explicitly require the staff members to proof their qualification by means of respective certificates. Concluding, IT-Grundschutz safeguards do not satisfy Technical Requirement 1 completely but provide a reasonable basis that can be adapted to the specific needs.

Technical Requirement 2 *can be completely satisfied by IT-Grundschutz.*

This technical requirement considers the assessment of residual security risks. For this purpose IT-Grundschutz implements a suitable approach. The procedure includes a supplementary security analysis and a subsequent risk analysis (see [62] for an introduction). The corresponding standard "Risk analysis based on IT-Grundschutz" describes the risk assessment procedure in detail (see [63]). The single steps include preparing a threat summary, determining additional threats, the threat assessment and the handling of risks. In this process residual risks are determined and documented. This documentation satisfies the requirement. If available, other documentation on remaining security risks of specific components, possibly from the manufacturer, is to be included as well. In Section 6.2 we give recommendations how to apply this procedure in the VSP scenario.

Technical Requirement 3 *can be completely satisfied by IT-Grundschutz.*

This requirement concerns the availability of the voting system. Ensuring the availability is a task for the operational environment. The technical requirement demands high-availability systems, backup systems and redundant components. The availability concerns primarily the voting server and the external network to guarantee that voters can access the voting system to cast their vote. Regarding redundancy and backup also structural components like the computer center and the server room, the whole network and the database for the storage of election data have to be considered. We map these components to suitable IT-Grundschutz modules. The use of a high-availability architecture for servers is implemented by safeguard S 2.314 from the module B 3.101 for general

servers. The module B 3.301 for security gateways ensures the high availability of the external network connections (S 2.302). Safeguards like backup systems and redundant components are provided for all related components. We start by considering structural components with the module B 2.9 for computer centers and the module B 2.4 for the server room. They implement safeguards for secondary and uninterruptible power supply (S 1.56, S 1.28) and redundancies in the technical infrastructure of server rooms (S 1.52). The module B 4.1 for the network guarantees the redundant arrangement of network components (S 6.53). Data backup safeguards are implemented for the whole network (S 6.52), for specific network components like routers and switches (B 3.302, S 6.91), and for the database (S 6.32, S 6.49). Handling data backups on the general level like the development of a data backup policy is ensured by the generic module B 1.4. Based on these safeguards the requirement for availability can be satisfied.

Technical Requirement 4 *can be completely satisfied by Common Criteria and IT-Grundschutz.*

This requirement considers procedures in case of interruption of the voting system. First we look at the voting software. The objectives O.Failure and O.OneVoterOneVote of the Common Criteria PP for online voting products [64] require the voting software to enable a secure restart after shutdown or crash while maintaining the integrity of election data and sustaining the legal election principles. Moreover, O.Failure ensures that the voting software provides the functionality to execute self tests. This can be used at request by the Election Host. In addition, O.OneVoterOneVote ensures that no voter is enabled to cast two votes after a restart of the voting procedure. The obligation to inform the Election Host of interruption is an organizational requirement. Here the generic IT-Grundschutz module B 1.8 for handling security incidents implements suitable safeguards to realize procedural rules and reporting channels for security incidents and the notification of affected parties (S 6.60, S 6.65). In addition safeguard S 6.11 from the module B 1.3 for contingency planning implements the necessary steps to restart an IT system after failure. Thereby the technical requirement is completely fulfilled.

Technical Requirement 5 *can be completely covered by Common Criteria and IT-Grundschutz.*

This requirement deals with emergency procedures. On the software side, the PP provides the objective O.Failure which ensures secure restart of the voting system in case of failures and exceptions. The integrity of the election data is maintained. Regarding the operational environment of the VSP, contingency planning concerns both the organization and the technical components. First we consider the organizational safeguards. By implementing the module "B 1.3 Contingency planning concept", a VSP analyzes the effects of failure of critical components in its IT systems in advance and specifies procedures for maintaining or restoring their availability. This includes technical failures as well as failures which are caused intentionally or as a result of negligence

(see [59]). Most important the module involves the development of contingency plans for selected incidents (S 6.9) as well as a post-incident recovery plan (S 6.11). To restore system availability after failure safeguard S 6.14 draws a plan how to replace components quickly. The module B 1.8 focuses on the handling of security incidents in order to maintain IT security in ongoing operations. In this context security incidents are defined as events which can have an impact causing major loss or damage, affecting integrity, confidentiality or availability of data (see [59]). Among many others, this comprises the establishment of a management system for handling security incidents (S 6.58) and the specification of responsibilities for dealing with security incidents (S 6.59), which includes assigning a security incident team (emergency service).

IT-Grundschutz also provides emergency safeguards for specific technical components. Since the effects of emergencies can be widespread, we consider the building as well as the components of the voting system according to the generic VSP architecture from Chapter 2. Module B 2.1 requires alert plans and fire drills for the building (S 6.17). For server rooms (module B 2.4), hand-held fire extinguishers (S 1.7), a hazard alert system (S 1.18), the avoidance of water pipes to prevent flooding (S 1.24), overvoltage protection (S 1.25), emergency circuit-breakers (S 1.26), local uninterruptible power supply (S 1.28), fire protection of patch panels (S 1.62), and smoking bans (S 2.21) are implemented. For servers (B 3.101), security gateways (B 3.301), routers and switches (B 3.302), IT-Grundschutz requires specific contingency planning (S 6.96, S 6.94, S 6.92). For the network (B 4.1) and the database (B 5.7) there exist several emergency safeguards ensuring integrity and availability by redundancy and backup systems.

At last, we consider safeguards for network problems resulting from malware or attacks. The generic IT-Grundschutz module B 1.6 requires the VSP to provide a computer virus protection concept and to install protective software on all threatened components (S 2.154, S 2.156). To secure the external network interface, modules B 4.1 and B 3.301 require the secure configuration of active network components (S 4.82) and a protection against DNS spoofing (S 5.59). The prevention of insecure network access is implemented in the general module for hardware and software management (B 1.9, S 2.204). Concluding, the IT-Grundschutz emergency safeguards are able to fulfill this technical requirement.

Technical Requirement 6 *can be completely satisfied using Common Criteria and IT-Grundschutz.*

This requirement concerns the following major aspects: confidential transmission of data, confidential storage of data, and access control for the voting server. Regarding the VSP's architecture, this involves the voting server and the internal and external network for data transmission, the voting server for storage, as well as the building and server room for physical access protection. Now we consider how each aspect can be satisfied. PP-certified voting software satisfies the objectives O.SecrecyOfVoting, O.SecretMessage and O.AuthenticityServer. They achieve the confidentiality of identification, authentication and the secrecy of ballot data during transmission. In addition,

IT-Grundschutz proposes mechanisms for securing data transmission in its generic module "B 1.7 Cryptographic concept" which is implemented during the IT-Grundschutz procedure. It includes the usage of cryptographic mechanisms like encryption, checksums and digital signatures (S 4.34) and most important the use of SSL (S 5.66). The use of encryption procedures for network communications is also ensured in safeguard S 5.68 of the module B 1.9 for hardware and software management. Concluding confidential transmission of identification, authentication and ballot data can be ensured.

Regarding the confidential storage of data, IT-Grundschutz safeguards from the generic module for archiving (B 1.12) can be implemented. This includes the selection of a suitable archive system (S 4.168) which involves data encryption, as well as the use of appropriate archival media (S 4.169).

Access protection comprises logical and physical protection. Both can be satisfied using IT-Grundschutz. The module "B 1.1 Organisation" provides safeguards to design access control policies for granting of site access authorizations (S 2.6), granting of system/network access authorizations (S 2.7), and granting of application/data access authorizations (S 2.8). The module also ensures the division of responsibilities and separation of functions (S 2.5) which can be used to define that access to the server requires two simultaneous users. Here the PP objective O.AuthElectionOfficers ensures that specific actions require the authentication of at least two election officers (VSP personnel in our scenario). These actions are: starting, restarting or ending the voting phase, and starting the tallying procedure. The generic IT-Grundschutz module B 1.9 ensures developing guidelines to control the access to IT components which includes the management of access rights (S 2.220). Regarding the voting server, safeguard S 2.204 prevents insecure network access. The gateway for the external network is protected by intrusion detection and intrusion response system (B 3.301, S 5.71). The physical access is controlled at the structural level. The modules B 2.1 for buildings and B 2.4 for the server room implement entry regulations and controls (S 2.17), closed windows and doors (S 1.15), locked doors (S 1.23), a key management (S 2.14), and moreover protection against break-in (S 1.19) and the use of safety doors and windows (S 1.10). We conclude that the technical requirement can be satisfied using the introduced objectives and safeguards.

Technical Requirement 7 *can be partially satisfied by Common Criteria and IT-Grundschutz.*

The identification and authentication of the voters is basically achieved by the voting software. The objectives O.UnauthorisedVoter, O.AuthenticityServer and O.OneVoterOneVote of the Common Criteria PP satisfy most aspects of this technical requirement: O.UnauthorisedVoter ensures that only eligible and correctly authenticated voters are allowed to cast their vote. O.AuthenticityServer ensures a trustworthy connection between the voters and the election server with secure mutual identification. O.OneVoterOneVote ensures only one vote per eligible voter which prevents multiple voting. IT-Grundschutz provides safeguards in order to determine appropriate authentication methods and select

suitable cryptographic products in the generic modules "B 1.7 Cryptographic concept" and "B 1.9 Hardware and software management" (S 2.164, S 4.133). The latter one implements authentication mechanisms based on PIN/TAN, tokens, or biometry. However, the requirement for two independent securing means for authentication is neither covered by the PP nor by IT-Grundschutz. The secure handover of the securing means has to be realized by the operational environment. Depending on the deployed voting system, such authentication means can be simple PIN/TAN letters, electronic soft tokens containing digital certificates or electronic devices like smart cards. Hence the methods for delivering those means may vary. While soft tokens could eventually be delivered via (secure) email, smart cards need to be sent via postal mail or the voters need to collect their authentication means personally at the VSP's. Consequently it is not possible to define general measures for delivery. Still IT-Grundschutz provides several safeguards which can be used to determine a secure strategy. The module B 5.2 defines comprehensive procedures for the exchange of data media (especially S 2.45 Controlling the exchange of data media, S 5.23 Selecting suitable types of dispatch for data media, S 2.44 Secure packaging of data media, S 3.14 Briefing personnel on correct procedures of exchanging data media). During evaluation, the responsible authority has to check the implemented measures for their suitability. The secure storage of the identification and authentication means is covered by IT-Grundschutz safeguards of the module "B 1.12 Archiving". The included safeguards ensure the electronic archiving, the selection of a suitable archive system and the use of appropriate archival media (S 4.168, S 4.169, S 2.242).

Technical Requirement 8 *can be completely satisfied by Common Criteria and IT-Grundschutz.*

This requirement deals with the integrity of election data which is handled by both the voting software and the operational environment. PP-certified voting software achieves the objectives O.IntegrityMessage, O.ArchivingIntegrity, O.IntegrityElectionOfficers and O.Failure. They ensure that election and authentication data (including identification data, the authentication message, ballot, vote records, ballot data and the acknowledgment) cannot be modified covertly during transmission between voter and server-sided voting system, they ensure the integrity protection of stored election data after tallying in a verifiable way, they protect the votes from modification by election officers (in our scenario the VSP's personnel) and ensure the verifiable integrity of election data after failure. The objectives O.Failure and O.OneVoterOneVote satisfy the requirement FDP_SDI.2.2 which ensures the reporting of data integrity errors to election officers (in the our scenario this is the VSP's personnel) (see [64, p. 54]). Thus alteration is detected. IT-Grundschutz provides additional safeguards in order to ensure data integrity. The relevant components are the communication channels as well as the voting server and the database. Appropriate cryptographic mechanisms for establishing integrity-protected communication channels are provided in the generic module "B 1.7 Cryptographic concept" (S 4.34 Using encryption, checksums or digital signatures, S 5.66 Use of SSL) as

well as the use of encryption procedures for network communications (B 1.9, S 5.68). The alteration of data on the voting server is detected by the safeguard S 4.93 for regular integrity checking. It is implemented following the module for general servers (B 3.101). The module B 5.7 explicitly ensures the integrity of the database containing the electronic votes (S 2.130) and provides procedures in case of a loss of database integrity (S 6.48). General loss of data is prevented the data backup policy implemented by module B 1.4. Concluding, this requirement is satisfied by the introduced Common Criteria objectives and IT-Grundschutz safeguards.

Technical Requirement 9 *can be partially satisfied by Common Criteria and IT-Grundschutz.*

The initial installation of the election data into the voting system must be realized by the operational environment. In our generic VSP model the initial election data is transfered to a database. Here the corresponding IT-Grundschutz module for databases (B 5.7) provides the safeguard S 2.135 that implements the secure transfer of data to a database. Thereby the requirement is satisfied. Setup and configuration of the voting server is realized by IT-Grundschutz safeguards. For the voting server we consider the module B 3.101 for general servers. It implements safeguards for planning the use of a server (S 2.315), the secure installation of a server (S 2.318) as well as the secure basic configuration of the IT system (S 4.237). It is complemented by the module B 5.4 for web servers which ensures the secure set up of a server for web services (S 2.175). Regarding the database which is used on the voting server the module B 5.7 implements the safeguard S 2.125 for the installation and configuration of a database. However these safeguards do not consider the specific configuration details for voting servers like for example the ballot details. Further adaption is necessary. Therefore we conclude that the safeguards only provide partial satisfaction of the requirement.

Technical Requirement 10 *can be completely satisfied by Common Criteria.*

This requirement is concerned with an interface for the Election Host to execute specific tasks. This is realized by the voting software. Implementing the PP objectives O.AuthElectionOfficers and O.Failure ensures that the voting software allows election officers executing specific tasks (in the current technical requirement this is the Election Host). O.AuthElectionOfficers requires the identification and authentication of the election officers before any action can be executed. In particular, the actions starting, restarting (also after technical failure), and ending the voting phase as well as initiating the tallying are provided. Following the rules 1–4 of the underlying security functional requirement FDP_IFF.1B.2 the voting software sets the corresponding attribute "election period" such that the action "starting" can only be executed once and ending the election sets the attribute to the value "tallying" which prevents further starting or restarting actions (see [64, p. 52]). Moreover, initiating the tallying is only possible when the attribute is set to "tallying" which means that the voting phased must have been

ended before. O.Failure ensures the technical preconditions for a restart after exceptions like crash or shutdown of the server-sided voting software, or after a communication or storage medium failure. In all cases the server-sided voting software enables the election officers (here the Election Host) to restart the voting phase. Concluding the technical requirement is fully satisfied.

Technical Requirement 11 *can be completely satisfied by Common Criteria and IT-Grundschutz.*

This requirement deals with initial checks of the voting system prior to the election start. It involves the voting software and the operational environment. The Common Criteria PP contains the objectives O.Tallying and O.Failure. Implementing O.Failure enables the election officers (for this requirement this would be the Election Host in the VSP scenario) to check the system status and execute self tests at initial start-up and at request. The self tests are set up to identify technical failures with respect to the integrity of the security functionality of the voting software or the user and system data which endanger the correct operation of the voting software. According to [64, p. 68] indications of such malfunctions are raised to the election officers by means of the component FDP_SDI.2 (in our scenario this would be the VSP's personnel). O.Tallying ensures that the ballot box is empty before tallying. The generic IT-Grundschutz module B 1.9 for hardware and software management ensures the secure erasure off previous data by implementing the safeguard S 2.167. It provides comprehensive mechanisms like formatting, overwriting, or destruction of data media and hard disks. Therefore the requirement is fulfilled.

Technical Requirement 12 *can be completely satisfied by Common Criteria.*

This requirement is concerned with the closure of the voting phase. This is handled by the voting software. The PP objective O.EndOfElection ensures that there is a time frame set that allows all ongoing casting procedures to be finished (taking into account the delay of data transport) while new voting processes cannot be initiated anymore (see [64, p. 67], in particular FDP_IFF.5.1 d)). As we already considered above in Technical Requirement 10, the component FDP_IFF.1B (included in O.EndOfElection) ensures that after ending the voting phase it is not possible to open or continue a voting process or to restart the voting system. Next, O.EndingElection ensures that "the election officers receive a notification in case they try to end the polling phase ahead of time. Following an explicit confirmation, the election officers are able to end the election even before the planned ending time of election." In our scenario it must be ensured that this functionality is made available to the Election Host. Concluding, the Technical Requirement is fulfilled by accordingly certified voting software.

Technical Requirement 13 *cannot be satisfied by Common Criteria or IT-Grundschutz.*

This requirement regards the representation of the electronic ballot. It is not fulfilled by neither the PP nor IT-Grundschutz. We assume that this is due to the fact that the requirement is more related to usability than to security which is the focus of Common Criteria and IT-Grundschutz. The VSP has to configure the voting system in a way such that the ballot representation conforms with the legal provisions given in this technical requirement, the correct implementation is to be checked during the evaluation procedure.

Technical Requirement 14 *can be partially satisfied by Common Criteria.*

The specific ballot casting requirements are mainly addressed by the voting software. In the Common Criteria PP we first identify the objective O.UnauthorisedVoter to suit the context of this technical requirement. It ensures the identification and authentication of voters as a prerequisite to cast a vote (see also [64, 1.2.4.4] for a more detailed description of the corresponding functionality of PP-compliant voting software). Thereby the requirements 1 and 2 are satisfied. However, the PP does not explicitly require the voting software to enable the voter to intentionally cast an invalid vote. Therefore requirement 3 is not necessarily satisfied by PP-certified voting software. Next, O.Abort ensures that a voter can abort the voting process at any time without losing his right to vote. In addition, the objective O.OneVoterOneVote ensures that the right to vote is preserved in the event of an abort caused by the voter, by technical means such as a timeout or communication errors or a restart of the voting phase. Thereby requirement 4 is satisfied. The objective O.Correction enables the voter to correct his vote any number of times until the final voting decision is cast. This satisfies requirement 5. Next, the objective O.Acknowledgement ensures that the voter is presented an acknowledgment regarding, amongst others, the successful storage of the vote in the electronic ballot box. The voter can access this information also later on after successful logging onto the voting system. Thereby requirement 6 is satisfied. The objective O.Proof prevents the voting software from making any information available to the voter that could be used to prove his voting decision to others. In particular, the information flow of votes, vote records, identification data, authentication message, ballot, ballot data, acknowledgment regarding the successful vote casting, vote-casting annotation or intermediate result is ensured not to enable the voter to prove his vote. (see [64, FDP_IFC.1A e), p. 49 and FDP_IFF.5.1 a), p. 53]). Moreover, the objective O.SecrecyOfVoting ensures that votes are not transmitted in clear text in order to prevent linking the voter with his vote. Neither the number of messages nor their size provides information on the number of crosses and/or on the invalid vote [64, p. 67]. Finally, O.ArchivingSecrecyOfVoting prevents to link a voter to his vote via the sequence of votes in the ballot box. Thereby requirement 7 is satisfied. The requirement 8 is not satisfied by neither PP objectives nor IT-Grundschutz. Coordinating different voting channels is primarily an organizational issue which has to be dealt with by the VSP's operational environment by implementing additional measures that have to be explicitly evaluated by the responsible authority.

Technical Requirement 15 *can be partially satisfied by Common Criteria and IT-Grundschutz.*

This requirement is concerned with the integrity and verifiability of the tallying procedure. This is addressed by both the voting software and the operational environment. PP-certified voting software fulfills the objective O.Tallying. It ensures the correct counting of all votes (see especially [64, FDP_IFC.1B.1 d), p. 52]). The authenticity and completeness of votes is ensured because votes are only accepted from authenticated voters due to the objective O.UnauthorisedVoter, and O.Tallying guarantees that the ballot box is empty at the beginning of the voting phase. Moreover, O.StartTallying ensures that the tallying cannot start before the completion of the election. The objectives O.Failure and O.ArchivingIntegrity ensure the integrity and verifiability of votes as well as the checking of election data integrity on demand (see also [64, 1.2.4.3, p. 17]). In particular, O.Failure protects the integrity of election data including votes and allows checking the integrity on request. O.ArchivingIntegrity guarantees that the integrity of the election data including votes is protected by means that are effective even outside the control of the voting software and that makes further manipulation detectable. We point out that while these objectives ensure accurate tallying and verifiable protection of the integrity of the election result, they do not explicitly ensure that every single step of the tallying process can be verified and reproduced. This requirement is of great importance for the election principle of the public nature of elections (see Chapter 4.4.2).

Next we consider how IT-Grundschutz safeguards contribute to satisfy the technical requirement. Following the generic module B 1.7 a cryptographic concept is established which includes using checksums and digital signatures for protection and verification of data integrity (S 4.34). In our generic VSP model we assume the tallying process to be executed on the voting server. The corresponding IT-Grundschutz modules for general servers and web servers (B 3.101 and B 5.4) require the implementation of safeguards for regular integrity checking (S 4.93) and the protection of data against subsequent changes (S 4.99). Moreover we assume the electronic votes to be stored in a database. The corresponding module B 5.7 ensures the integrity of the database (S 2.130). These general safeguards can be used to ensure the integrity of the votes on the server.

To ensure that the tallying software is unaffected by other applications, we consider collusion of components or attacks on the network level. The IT-Grundschutz module B 4.1 for the network provides safeguards in order to achieve logical or physical segmentation of components (S 5.61, S 5.62) or to audit the network in order to detect malicious collusion (S 4.81). The generic module B 1.6 sets up a computer virus protection concept to protect the voting software from malicious software (S 2.154, S 2.156). At last, we consider the requirements for alternative tallying software and public initiating of tallying. They are not satisfied by neither PP-certified voting software or IT-Grundschutz safeguards. The voting software has to be adjusted in a way that the data structure can be interpreted by other applications. Public initiating of tallying is an organizational issue that could be realized by the VSP's personnel.

Technical Requirement 16 *can be partially satisfied by Common Criteria and IT-Grundschutz.*

This requirement deals with the election protocol which involves both the voting software and the operational environment. PP-certified voting software achieves the objective O.Audit and thus generates a protocol recording events and dates of the election. Thereby it satisfies the general requirement for an election protocol on the software side. However, the objective does not explicitly require the protocol to be verifiable. The auditing of network and server components can be achieved by IT-Grundschutz safeguards for monitoring complex client-server architectures including server computers. In our model we consider the basic components of the voting server, the network and the database for storage of votes. The corresponding IT-Grundschutz modules B 3.101, B 4.1 and B 5.7 provide respective safeguards for auditing these components (S 5.9 Logging at the server, S 4.81 Auditing and logging of activities in a network, S 2.133 Checking the log files of a database system, S 4.70 Monitoring a database). The whole VSP computer center (module B 2.9) including its server rooms can be monitored by implementing video surveillance systems (S 1.53). The secure storage and archiving of the election protocol data is satisfied by implementing the generic IT-Grundschutz modules for archiving (B 1.12) as well as a data backup policy (B 1.4) for implementing backup systems to restore stored data. We point out that according to the legal regulation the VSP is not responsible for long-term archiving of election data. According to VSP Act §10 (2) (explanatory memorandum) it is the Election Host that is responsible for the secure storage of the election protocol data for the period designated in the particular election provisions (see [92]). This regulation relieves the responsible authority from its duty to take over the election protocol data in case of withdrawing the accreditation or abandoning of operation of a VSP. Hence no special safeguards in this matter beyond IT-Grundschutz are necessary. The requirement for a correct system time source is fulfilled by implementing the IT-Grundschutz safeguard for a local NTP server for time synchronization (S 4.227). A time stamp service according to S 5.67 can be used to provide the time stamps required for recording events and actions in the election protocol.

Regarding the contents of the election protocol, the objective O.Audit requires the voting software to include the following information:

- Successful identification and authentication of the election officer
- Starting, restarting and ending of the polling phase
- Starting of tallying with determination of the election result
- Performance and results of every self-test
- Identified malfunctions in the use of supporting mechanisms from the IT environment which compromise the operational capability of the server-sided voting software

This list can be supplemented [64, 1.2.4.7, p. 20]. The VSP must ensure that all data which must be recorded according to this requirement are added to the list. O.Audit specifically includes date and time of each event, the type of event, the subject identity (without information on the identity of the voter), and the outcome (success or failure) of the event (see [64, FAU_GEN1.2, p. 48]). Thereby this part of the requirement is satisfied.

Regarding the protection of the election protocol, voting software certified according to the PP implements O.ArchivingIntegrity and O.Failure. Thereby the protocol data are protected against manipulation, subsequent manipulation can be detected. Moreover certified voting software allows checking of the data integrity and ensures data integrity after system failure and interruption. Regarding the operational environment we consider the voting server which is supposed to store the election protocol. The generic module IT-Grundschutz module B 1.7 for a cryptographic concept and the module B 3.101 for general servers implement the safeguards S 4.34 for using encryption, checksums and digital signatures as well as S 4.93 for regular integrity checking. Thus they provide additional mechanisms to ensure the protocol integrity. The safeguard S 5.9 of the module for general servers logs in particular any attempts to gain unauthorized access to the server and thereby ensures tamper-evidence. However there are some specific requirements which are not completely satisfied by PP objectives or IT-Grundschutz safeguards like for example the usage of qualified signatures to sign the election protocol data. Moreover, there is no PP objective or IT-Grundschutz safeguard which ensures that the protocol data can be processed by commercially available data processing systems. This includes the requirement to enable the reproduction of the election result.

O.Audit ensures that the election protocol does not include information which might endanger the secrecy of the vote since no information on the voter's identity is recorded (see [64, FAU_GEN1.2, p. 48]).

Access protection is realized by IT-Grundschutz safeguards. The generic module "B 1.1 Organisation" regulates the granting of access authorizations for applications and data (S 2.8). Access to the building and the server rooms is protected by module B 2.1 and B 2.4 which implement appropriate entry regulations and controls (S 2.17). The generic module B 1.9 for hardware and software management implements guidelines for access control on the hardware and software level and prevents insecure network access (S 2.220, S 2.204).

Technical Requirement 17 *can be completely satisfied by Common Criteria and IT-Grundschutz.*

This requirement regards the anonymity of the votes. It involves the voting software and the operational environment. For PP-certified voting software, the objectives O.SecrecyOfVoting, O.SecretMessage, O.ArchivingSecrecyOfVoting, O.SecrecyOfVotingElectionOfficers and O.Proof ensure anonymity throughout casting, transmission, storing and tallying of the votes. In more detail, O.SecrecyOfVoting and O.Secret-

Message ensure that the secrecy of voting during transmission is guaranteed by using a secure communication path, that prevents a link between the voter and his vote. No conclusions on the number of crosses and/or their position and/or on the invalid vote, can be drawn from the number or size of the messages. O.ArchivingSecrecyOfVoting ensures that the data stored on the election server after the determination of the election result cannot be used to link the voter to his vote. This holds in particular after breakdowns. The construction of a link between a voter and his vote is in particular not possible based on the order and/or the time when the vote record was stored in the ballot box. O.SecrecyOfVotingElectionOfficers ensures the secrecy of voting at the voting server during the voting phase and the tallying. A reconstruction of the link between voter and his vote is not possible for the election officers (in our scenario the VSP's personnel). O.Proof ensures that the voter himself cannot proof his voting decision to others. The secure erasure of election specific data on the vote-casting device can be achieved by implementing the IT-Grundschutz safeguard "Secure deletion of data media" (S 2.167) in the voting software. This safeguards is part of the generic module B 1.9 for hardware and software management which must be considered for all IT infrastructures certified according to IT-Grundschutz. The safeguard describes methods to securely erase data, for example by overwriting files.

Technical Requirement 18 *can be partially satisfied by IT-Grundschutz.*

The briefing of the Election Host is an organizational issue for the VSP. The PP does not require the voting software to provide any briefing functionality. However the briefing can be realized by implementing IT-Grundschutz safeguards. Among the generic IT-Grundschutz modules are B 1.2 for personnel and B 1.13 for IT security awareness and training. They include safeguards to train new staff with their work (S 3.1), to make staff aware of IT security issues (S 2.198), to train before actual use of a program (S 3.4), to train on IT security safeguards (S 3.5), and to instruct staff members in the secure handling of IT (S 3.26). However these IT-Grundschutz safeguards are mostly intended for the briefing of personnel and do not contain election specific instructions. They have to be adapted accordingly and all required points have to be included in the briefing.

Technical Requirement 19 *can be partially satisfied by IT-Grundschutz.*

The briefing of the voters needs to be jointly realized by the voting software and the operational environment. Basically the IT-Grundschutz safeguards from the Election Host briefing are applicable (see Technical Requirement 18). These safeguards provide a basis to inform and instruct the voters. Still, it has to be extended and adapted to the election scenario. All specific election related information from the technical requirement have to be included. The adaption also has to include that the textual instructions are compliant with §126 German Civil Code [4]. The voting software has to provide a function which requires the voter to confirm taking note of the instructions prior to

voting. This is not covered by PP-certified voting software. However, Application Note 13 of the PP explicitly allows for such a procedure [64, p. 18]. This could be addressed by the software manufacturer. At last, the VSP is required to provide a help desk. This can be realized using IT-Grundschutz safeguards. The generic module B 1.9 for hardware and software management implements services and counseling for IT users (S 2.12) by means of establishing a central contact unit. The generic module B 1.13 for IT security awareness and training ensures that contact persons for security questions are made available (S 3.46). Thereby the requirement for a help desk is satisfied.

Technical Requirement 20 *can be partially satisfied by IT-Grundschutz.*

The documentation of adherence to the law is not explicitly considered in the PP or in IT-Grundschutz and hence is not completely satisfied. Still there are IT-Grundschutz safeguards which can satisfy the technical parts of the requirement. The integrity of the documentation data is protected by implementing the generic IT-Grundschutz module B 1.7 that establishes the cryptographic concept. It includes the use of encryption, checksums and digital signatures (S 4.34). The secure storage and archiving of the documentation is ensured by the generic module B 1.12 for archiving. It describes planning and design, procurement, implementation and operation as well as contingency planning for an archiving system. The module explicitly considers the implementation of legal provisions (S 2.245). The VSP must ensure that the corresponding safeguards are implemented accordingly, in particular to achieve the requirement for long-term storage for a period of 30 years.

Technical Requirement 21 *can be completely satisfied by IT-Grundschutz.*

The requirement of data protection is fulfilled by IT-Grundschutz if the module B 1.5 for data privacy protection [14] is implemented. The module comprises technical and organizational safeguards and ensures compliance with the relevant German laws for data protection including the German Federal Data Protection Act [6] or data protection acts of the states depending on the application scenario [14, p. 1]. The safeguards include the development of a data protection concept (S 7.3), technical-organizational controls for the processing of personal data (S 7.4), awareness training of personnel (S 7.6) as well as maintenance and documentation measures.

Data protection is a very specific field in IT security that attracted more and more attention lately, especially in Germany and other European countries. In this context, audit methodologies have emerged that are specialized solely in data protection. While IT-Grundschutz basically is sufficient these methodologies could be used as an alternative, for example if a VSP already has a corresponding certificate. The German "Independent Centre for Privacy Protection Schleswig-Holstein (ICPP)" is a cooperation of evaluation authorities specialized on data protection audits [13]. These authorities perform legal and technical checks on the product or system to verify its conformance with the data protection regulation. In case of positive results the ICPP awards a 'Pri-

vacy Seal'. An ICPP data protection audit has already been performed in the field of electronic voting for the German "dotvote" voting system [50]. The European Privacy Seal ("EuroPriSe", see [2]) allows for data protection audits of IT products and services based on European data protection regulations, especially the "European Data Protection Directive" (95/46/EC) [52] and the "European Directive on Privacy and Electronic Communications" (2002/58/EC) [53]. The evaluation criteria have been laid down in a catalog [1]. EuroPriSe extends the ICPP approach to the European context. In Germany the responsible certification authority is again the ICPP. The EuroPriSe could especially be useful if a VSP intended to operate across European borders.

6.2. Results and Recommendations

Our analysis revealed that eleven technical requirements of the Security Concept Template can be completely satisfied, nine requirements can be partially satisfied and only one requirement cannot be satisfied by the security objectives of the PP for online voting products or by IT-Grundschutz safeguards. We illustrate this result in Figure 6.1.

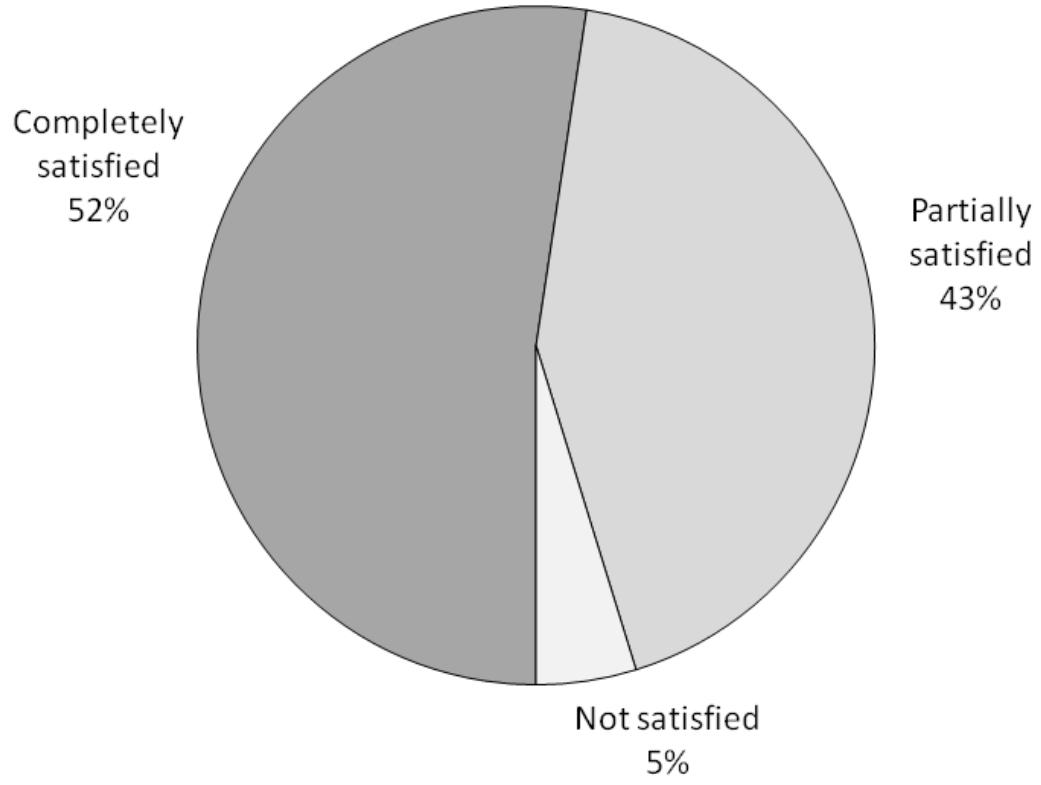

Figure 6.1.: Satisfaction of the technical requirements by PP security objectives and IT-Grundschutz safeguards

In other words, the majority of requirements can be completely or at least partially satisfied if the VSP uses PP-certified voting software and has its operational environment

certified according to IT-Grundschutz such that the referenced safeguards are included in the certificate. Concluding the proposed methodologies are indeed applicable to the VSP evaluation. If a VSP already owns corresponding Common Criteria or IT-Grundschutz certificates the remaining evaluation effort is greatly reduced. We point out that these results may vary for specific election scenarios with different protection requirements.

Now we recommend a procedure to deal with the technical requirements that are not completely satisfied according to our analysis. It is illustrated in Figure 6.2.

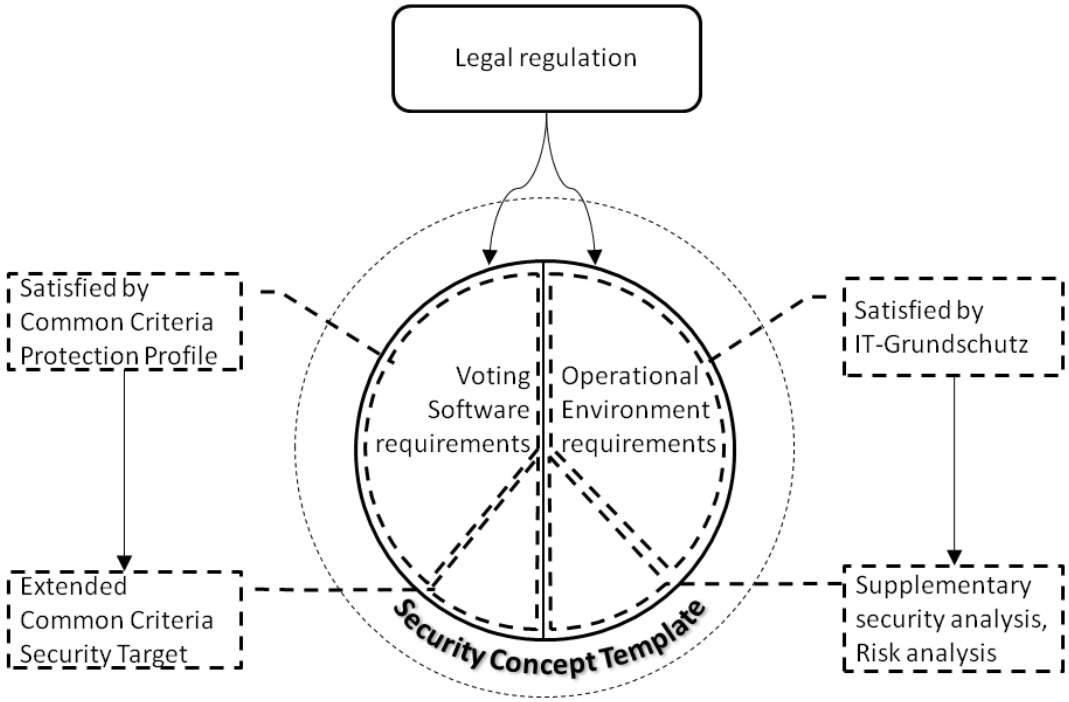

Figure 6.2.: Handling remaining requirements

First we consider Common Criteria. The technical requirements include a few for the voting software which are not sufficiently covered by the Protection Profile for online voting products. These requirements still need to be evaluated and certified if a VSP wants to be accredited. To solve the problem, voting software manufacturers could address the remaining requirements by adding corresponding security objectives to their Common Criteria *Security Target* in order to include them in the product evaluation. The Security Target is the basis for the Common Criteria evaluation of a concrete product. This document describes the security objectives for the specific product with all its special characteristics. The Security Target is to the product as the Protection Profile is to the product class. It represents a specific instantiation of the superordinate Protection Profile. Usually a Security Target claims conformance to such Protection Profile. In our case, it is possible to include additional security objectives in the Security Target because the Protection Profile for online voting products demands "strict conformance" of certified products (see [64, Chapter 2]). This means that compliant Security Targets "shall contain all security objectives (...) of the Protection Profile but may specify

additional security objectives" [23, Annex D.2]. Therefore suitable security objectives could be integrated in the extended Security Target for the voting software. We therefore recommend that manufacturers adjust the functionality of their voting software in order to satisfy all requirements of the Security Concept Template and correspondingly augment the security objectives in their Security Target. Accordingly certified voting software would proof not only conformance to the Protection Profile for online voting products but additional 'VSP-suitability'.

Next, we consider IT-Grundschutz. In order to deal with specific security requirements IT-Grundschutz provides the following approach. The *supplementary security analysis* is applied if certain components have higher protection needs, if components cannot be modeled appropriately due to the lack of respective IT-Grundschutz modules, or if components are deployed in an untypical way (see [62, p. 70]). In order to handle such special requirements IT-Grundschutz provides several options. First, optional "Z-safeguards" from the IT-Grundschutz catalog can be added to achieve a higher protection level (see [59, p. 19]). If not sufficient, an additional *risk analysis* needs to be performed. The intention is to determine threats to the IT infrastructure that are not considered sufficiently by the regular IT-Grundschutz safeguards and to find appropriate safeguards. The approach is described in [63]. Briefly it identifies additional threats and protection requirements, assesses the threat probability and the potential damage and finally determines measures to handle the risks. According to [62, p. 72], risks can be reduced by additional safeguards, risks can be avoided (e.g. by restructuring business processes), risks can be transferred (e.g. by insurance policies) and under certain circumstances (e.g. low threat probability upon extremely costly safeguards), risks can be accepted and therefore remain. Such residual risks must be assessed and documented in the "consolidation" process. For the VSP accreditation, residual risks are determined in any case because this step is legally required (see Technical Requirement 2 in Chapter 5). We recommend that the VSP performs the described supplementary security analysis and – if necessary – the risk analysis prior to the accreditation process in order to identify objects with higher protection requirements and developing appropriate strategies, for example improved safeguards. As a result of this procedure the VSP is able to determine for which components of its operational environment existing IT-Grundschutz certificates suffice and where additional evaluation is needed.

Following the described procedures the partially satisfied or unsatisfied technical requirements of the Security Concept Template can be included in a VSP evaluation and certification procedure based on Common Criteria and IT-Grundschutz. This finally confirms the applicability of these methodologies in the VSP scenario.

6.3. Accreditation

6.3.1. Procedure

The accreditation officially confirms the compliance of a VSP with the legal regulation after successful evaluation and certification. The procedure is introduced in the VSP Act

(see Chapter 4.1, Part 2). An accredited VSP is confirmed to satisfy all requirements of the Security Concept Template in order to provide secure and legally compliant online elections. Accredited VSPs can refer to their certified security in legal and business dealings. We briefly describe the accreditation procedure. The actors and their interactions are illustrated in Figure 6.3.

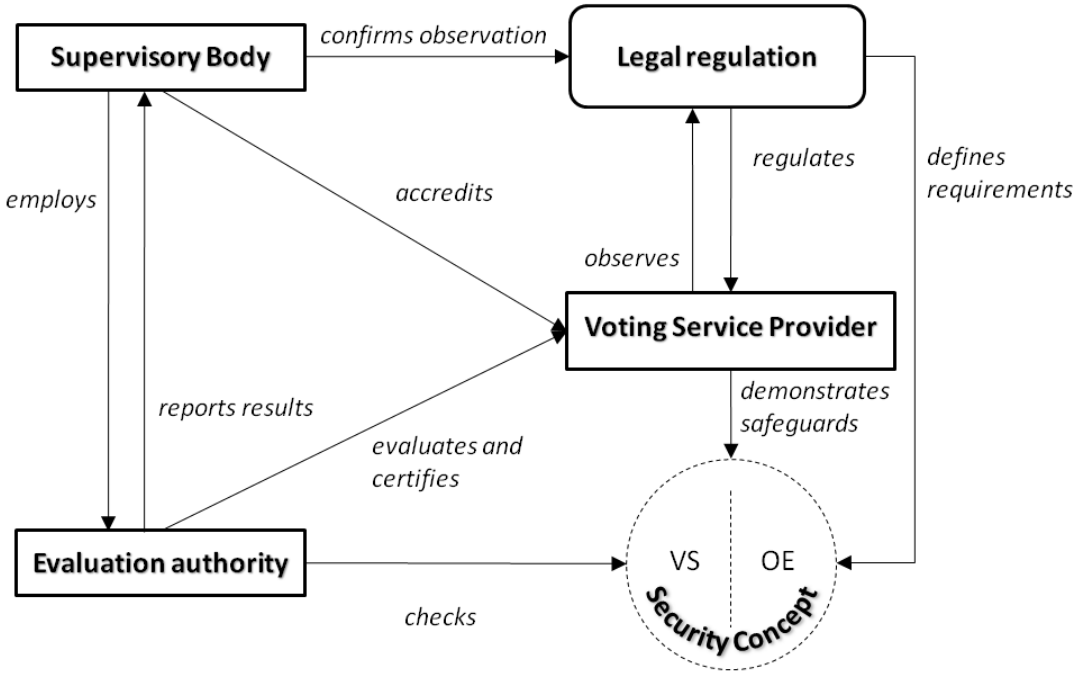

Figure 6.3.: Accreditation procedure

According to the VSP Act the accreditation is conducted by the Supervisory Body. It is authorized to delegate the performance of the evaluation and certification to private evaluation authorities. Their task is to evaluate and certify the VSP based on its Security Concept, for example using Common Criteria and IT-Grundschutz. The result is reported to the Supervisory Body which on that basis decides on the accreditation. If the decision is positive, the VSP will be accredited by the Supervisory Body.

We briefly introduce the possible testing levels of Common Criteria and IT-Grundschutz that could be used as the basis for the decision on accreditation. The Common Criteria provide seven *Evaluation Assurance Levels (EALs)* in order to classify extent and depth of the evaluation. EAL 1 restricts to basic functional testing. Semi-formal design and evaluation requirements are introduced with EAL 5. EAL 7 provides complete formally verified design and testing (see [24] for details). Of course costs and effort of such Common Criteria evaluation increase with higher EALs. In practice, a trade-off must be found. The Common Criteria evaluation methodology [25] provides detailed evaluation instructions only for EAL 1–4, with some additional information for higher levels [109]. In the commercial environment the EALs 1–4 are normally used [54]. IT-Grundschutz provides the *ISO 27001 certification based on IT-Grundschutz* which incorporates the

procedures and requirements of the ISO 27001 certification based on IT-Grundschutz safeguards (see [62, p. 87] for details). The certification procedure comprises inspection of the reference documents, on-site inspection, and generation of audit reports.

6.3.2. Choice of the Supervisory Body

In addition to the accreditation, the Supervisory Body has general supervision responsibilities[3] (see Chapter 4.1, Part 4, and [92]). It supervises the continuous observation of the legal regulation by VSPs. To this end, the Supervisory Body is authorized to take measures towards VSPs as well as evaluation authorities to ensure the observation of the legal regulation. Moreover the Supervisory Body supervises the abandonment of practice of a VSP and is responsible for the recognition of evaluation authorities. At last, according to article § 16 (3) of the VSP Act, the Supervisory Body is the responsible authority for prosecution of administrative offenses according to § 36 (1) of the German Administrative Offenses Act [12]. It is thereby empowered to impose fines or to prohibit operation in case a VSP violates the observance of the law. Thereby the Supervisory Body strengthens the trustworthiness and the secure operation of accredited VSPs.

Due to these important duties of the Supervisory Body it is an important question how to select an appropriate authority. In the similar context of the German Signature Law (see Chapter 3 and [102]), the responsible authority for supervision and accreditation of Certification Authorities (CAs) is the Federal Network Agency [8]. For evaluation and certification purposes the Federal Network Agency authorizes third parties, for example the German Federal Office for Information Security [9] and the TÜVIT [15]. Their qualification and experience in the context of CAs suggests employing them for the VSP scenario as well. However, in election scenarios it is most typical to have several parties with opposing interests involved. Depending on the election scenario, great care must be taken that the independence and neutrality of the Supervisory Body does not come in doubt [33]. Otherwise, the goal of trustworthiness may be compromised. The acting authorities should certainly not be involved in the realization of the election or its implementation by the VSP [80]. Official authorities could be seen as governmental intervention where it would be inappropriate. Nonetheless, we consider an official authority a reasonable approach to create trust in VSPs for non-political elections. Because here, an official authority is unlikely to have interest in the outcome of the elections and there is not much reason for collusion. In general it seems difficult to assign an authority completely independent with regard to all election scenarios. Private actors are profit organizations and might therefore raise suspicion regarding their independence. But even official bodies cannot guarantee impartiality, especially in political election scenarios. Barrat proposes academia as a possible neutral compromise, but this might be difficult to put into practice [33]. Furthermore, the author recommends involving non-governmental organizations or expert groups which could act as stakeholders to define strategies to promote transparency and public confidence. In any case, transparency of the evaluation and accreditation procedure should dramatically increase the trustworthi-

[3]Parts of this section can also be found in our publication [P3] with minor textual changes.

ness of both the acting authority and the process itself. Respective documentation, open evaluation criteria etc. should be publicly accessible. Moreover, independence could be enhanced by assigning different authorities for different types of elections. Another idea is for political elections to deploy several supervising authorities thereby sharing the control. This is an open question and subject for further research.

6.3.3. Protection Level

We briefly consider the protection level of the Protection Profile and IT-Grundschutz. In Section 6.3.1 we introduced the Common Criteria Evaluation Assurance Levels (EALs). The Protection Profile for online voting products is evaluated itself [64, 67]. Thereby it is certified to be complete, consistent, and technically sound and hence suitable for use as the basis for a Security Target. Since this Protection Profile requires 'strict conformance' of compliant Security Targets and products, they must satisfy at least the same statements as given in the Protection Profile [64, p. 22]. A compliant Security Target therefore would at least achieve the same EAL and so would do accordingly certified voting software [23]. The Protection Profile for online voting products is certified to comply with EAL 2+ [64, p. 22]. The "+" indicates that the level is augmented with additional assurance requirement modules from Common Criteria part 3 (for details see [24]). For evaluation in the field of electronic voting, even higher levels might be desirable. It seems reasonable to hinge the EAL on the targeted election scenario since for example parliamentary elections imply higher security requirements than non-political elections like the election of a works council. The Protection Profile for online voting products is intended for non-political elections with low attack potential [64, p. 7]. Therefore EAL 2+ is considered sufficient. We consider the non-political election scenario to be especially attractive for VSPs (see Chapter 2). Moreover the legal regulation for VSPs concentrates on non-political elections. Hence this EAL seems acceptable for the regular VSP scenario. The EAL for the VSP's voting software is supposed to be legally stipulated in the VSP Ordinance. VSPs which want to provide their online voting services even for political election scenarios may consider a higher EAL on a voluntary basis as long as these elections are not legally regulated otherwise. Such higher EAL could be reflected in an extended Security Target. In accordance with Volkamer and Grimm the required evaluation level could be increased to EAL 4+ depending on the intended application scenario [110]. The core of the system could even be evaluated according to the highest level EAL 7 if necessary. The specific EAL should be determined in joint work with technical and legal experts.

The safeguards from the IT-Grundschutz catalog ensure a "normal" security level for typical threats (see [62] for details). This might not be sufficient for all online voting scenarios. However, following our argumentation in the case of the Protection Profile, we consider a normal protection level an adequate basis for an accredited VSP in non-political election scenarios. The specific protection needs of the VSP's components can be identified during the IT-Grundschutz procedure. If there are higher protection requirements – possibly for parliamentary elections – IT-Grundschutz provides the supplementary security analysis and the risk analysis that we introduced before. Concluding

IT-Grundschutz provides appropriate instruments to adapt to the specific needs of VSPs.

6.3.4. Update of Security Mechanisms

Most online voting protocols make extensive use of cryptographic primitives to achieve the desired security properties. The corresponding algorithms not only include cryptographic standards like encryption, digital signature, and hash functionality. Moreover they comprise specific mechanisms for online voting systems (see [104] for an introduction). Examples are blind signatures, mix-nets, bulletin boards, homomorphic encryption or zero-knowledge proofs (see [34], [79], [86], [91] or [27] for corresponding protocols). However, the security level of such cryptographic primitives generally decreases over time due to new attacks and more powerful computers. Hence in order to ensure the continuous security such algorithms and their parameters must be checked periodically and adjusted or even replaced. This has to be addressed in the accreditation of VSPs. We consider how this can be done based on the legal regulation.

There are many sources that provide regularly updated information on recommended cryptographic algorithms and parameters. Examples are the yearly report of the European Network of Excellence for Cryptology II (ECRYPT II) [26], the publications of the National Institute of Standards and Technology (NIST) [32] or the recommendations from the French Network and Information Security Agency (FNISA) [56]. More information and additional sources can be found at BlueKrypt [35]. In Germany, recommended algorithms and parameters are listed in a regularly updated catalog published by the Federal Network Agency [69]. It defines the validity of algorithms and parameters for a specific time period. The use of these algorithms and parameters is legally stipulated for accredited CAs in Germany (see [102, §15 (7)] and [103, §17 (1)–(3), Annex 1 (I) no. 2]). Regarding the VSP scenario the situation is similar. Annex 1 (II) of the VSP Ordinance prescribes that cryptographic algorithms used by the VSP must satisfy the corresponding requirements of the German Electronic Signature Ordinance [92]. Hence accredited VSPs must choose current algorithms and parameters in accordance with the algorithm catalog for CAs [69]. Furthermore, article §3 (4) of the VSP Act prescribes that the accreditation must be repeated in case of substantial changes to the security of the VSP. This is the responsibility of the Supervisory Body which in such cases would instantly inform the VSPs about the need for action. Concluding the legal regulation for VSPs, the accreditation procedure, and the Supervisory Body provide the instruments necessary to ensure that accredited VSPs use secure and updated cryptographic mechanisms to the greatest possible extent.

However, the algorithm catalog of the German Federal Network Agency so far is limited to cryptographic primitives that are applied by CAs. While these are standard primitives that are used by VSPs as well, the catalog still lacks specific primitives for online voting. These have to be included in the catalog to ensure that all applied algorithms are up-to-date and secure. Compared to standard cryptography, specific primitives for electronic voting are mostly younger and therefore have not been analyzed and categorized in such a profound manner. There are first attempts to categorize these primitives, see for example [96] and [87]. Still a comprehensive catalog with recommendable parameters

confirmed by experts is not yet available. This is considered future work.

7. Design Proposal

In this chapter we provide an exemplary specification of a Voting Service Provider (VSP) based on a real election scenario. Thereby we demonstrate how to put the VSP into practice and proof the feasibility of the concept. To this end we refine our generic VSP model by embedding the technical and organizational safeguards we identified in the last chapter. The design proposal is the last building block of our security approach. This chapter is based on work we published in [P4].

7.1. Election Scenario

The specification of a VSP depends on the election scenario and the voting system in use. For our design proposal we therefore choose the scenario and the voting system of the Austrian Students Union[1] election in 2009 as a basis [40]. Since the Austrian election was non-political the scenario is in line with the legal regulation and the evaluation concept for VSPs. Choosing a real election scenario as background allows a VSP specification as realistic as possible.

Now we briefly introduce the election scenario. Detailed information can be found in [31]. The Austrian Students Union is the general university students' representative body in Austria [39]. It provides students with political and academic representation, information and service. The statutes of the Austrian Students Union are regulated in a federal law and an ordinance [17, 20]. Every two years all Austrian students are entitled to elect the representative bodies of the Austrian Students Union. The legal regulation explicitly allows for electronic voting [20]. For the 2009 election the students were enabled to cast their votes electronically via Internet, using their personal computers or alternatively computers in official polling stations. After the electronic election period, a second voting period based on classic paper based voting took place. Around 2200 students cast their vote over the Internet [105]. The voting software and hardware was implemented and operated at the Austrian Federal Computing Centre[2] [43]. For identification and authentication the students used their electronic Austrian Citizen Card[3] and respective card readers which were distributed at no charge.

[1] Österreichische Hochschülerinnen- und Hochschülerschaft, ÖH

[2] Österreichisches Bundesrechenzentrum, BRZ

[3] Österreichische Bürgerkarte, `http://www.buergerkarte.at/en/index.html`

7.2. Actors

The set of actors is the same as introduced in the generic VSP concept in Chapter 2. However we refine the generic model by including the corresponding safeguards from the IT-Grundschutz catalog (see [59]) that we identified in Chapter 6 to fulfill the specified requirements for VSPs. Moreover we adjust the description of the actors according to their specifics and tasks in the election scenario at hand.

Voting Service Provider The VSP's primary task is to technically implement the online election. For this purpose the VSP employs responsible personnel. To decide on their trustworthiness the VSP implements the IT-Grundschutz safeguards we identified for this purpose in the previous chapter. We briefly describe the procedures according to their description in the IT-Grundschutz catalog and reference the safeguards by their number in brackets (S x.xx). The full description can be found in [59]. The personnel's general qualification is checked based on their papers and interviews (S 3.50). The personnel then are trained to be able to perform the assigned duties based on a qualification policy that clearly defines the respective responsibilities (S 3.51). This holds in particular for the personnel that maintains and operates the voting system. They receive periodic training to be able to perform their tasks correctly and detect system failures (S 3.11). To ensure their availability at all time, qualified substitutes are appointed (S 3.10). The training first considers basic IT safeguards regarding personnel, products, procedures in case of malicious attacks or emergencies, backup procedures, or handling of personal data (S 3.5). Then the personnel is instructed in the specific configuration and operation of the voting software (S 3.4). The training is based on a plan that includes both the legal and technical aspects of IT security and the online voting system (S 3.45). To ensure reliability and trustworthiness of the personnel the VSP verifies their commitment to follow the legal stipulations by having them sign a receipt of the corresponding regulations (S 3.2). Moreover the personnel undergo a security vetting to confirm the adequacy and correctness of their academic and professional qualifications (S 3.33). They sign non-disclosure agreements (M 3.55) and provide up to date certificates of good conduct.

Another organizational issue that the VSP takes care of is access protection. Therefore the following IT-Grundschutz safeguards are implemented. To restrict access to the voting system and the election data to authorized persons the VSP lays down an access control policy (S 2.220). In a first step the VSP's functions are logically separated in order to define compatible sets of tasks that do not interfere. Then the corresponding responsibilities are assigned to respective personnel (S 2.5). On that basis, the protection requirements for access are determined and respective rights to access the site, the system and the network, and the applications and the election data, are granted to authorized persons (S 2.6, S 2.7, S 2.8). Access to the IT infrastructure, the server rooms, and the election data is limited to authorized VSP personnel with specific exceptions to enable authorized members of the Election Host, the voters and the public to access the voting system or the election data to the extent permitted or required by the law.

In compliance with our identified requirements the VSP ensures data protection

throughout its voting service. Established law on data protection is obeyed. To this end the VSP implements the previously identified IT-Grundschutz safeguards. It develops a data protection concept (S 7.3[4]). It contains the relevant points that have to be considered during organization and data processing. This includes the legal basis, procedures for data minimization, the rights of the users, logging and deletion techniques, a responsible data protection officer and many more. The VSP analyzes the specific legal requirements and checks whether the processing of personal data within its voting service needs to be adapted (S 7.4). The VSP personnel are trained in the meaning of data protection and sign official secrecy declarations (S 7.6).

Moreover the VSP is responsible for dealing with security incidents which might result in the loss of election data or damage. This can be caused by user errors, hacking attacks, or criminal acts (see [59, B 1.8]). To protect against these issues the VSP implements the following IT-Grundschutz safeguards from Chapter 6. Handling such incidents starts at the IT security management level. Here the VSP implements several steps in order to assess the situation and respond adequately (S 6.58). Basically it specifies a responsible security incident team and instructs the personnel throughout all levels on correct behavior (S 6.59). The personnel follow procedures and instructions based on typical incidents analyzed in advance (S 6.60). In order to be able to respond quickly, affected parties are notified following a predefined order (S 6.65). In addition the VSP develops a concept to restore system operability in case of contingencies that endanger the operation and the availability of the voting system. To this end a plan lists the necessary steps to be taken in order to recover after an incident or failure have occurred. This includes replacing components, restoring data transmission, re-installation and configuration and restarting of the system (S 6.11). Regarding replacement a concept considers possible component alternatives and the specific requirements how quickly a component needs to be replaced (S 6.14). The VSP defines procedures for emergencies like fire, water of power failure (S 6.9).

Election host The Election Host is represented by the electoral commission of the Austrian Students Union. It has the superior organizational responsibility for implementing the election according to articles §25 (2) of the Austrian Students Association Act and §2 and §35 of the corresponding ordinance [17, 20]. In our adapted scenario the electoral commission hires the VSP to technically implement the online election on his behalf.

Voters According to Austrian Students Association Act §35 (1) and §17 (2) of the ordinance, all students are entitled to vote despite their nationality [17, 20]. For the purpose of vote casting these voters connect to the VSP using Internet-enabled computers, for example their home PCs or kiosk systems [31, p. 018]. For assistance, the voters are enabled to contact the VSP on a support hotline.

[4]The safeguards for data protection can be found in the additional IT-Grundschutz module B 1.5 [14].

Public The public is everyone interested in the election. They are allowed to access information on the election procedure published on the VSP's Internet portal. Such information are for example the list of proposed candidates as well as the election results.

7.3. Architecture

In this section we describe the VSP's hardware and software, the network infrastructure, as well as the building and rooms in which the voting servers are located. The architecture is specialized from the generic VSP model in the following sense: First, the generic setup is expanded by the components and safeguards from IT-Grundschutz that we identified in Chapter 6. And secondly, the architecture reflects the specific setup that is required by the voting system in use, in this case the Pnyx.Core system from Scytl that was used in the Austrian election [99, 40]. An overview of the architecture is visualized in Figure 7.1.

Remark. We point out that the voting software described in this design proposal partially differs from the original Pnyx.Core scheme. The Scytl software was used only for our guidance. We used the information publicly available in [99], modified the scheme and adapted it to the VSP scenario. Therefore the IT architecture and the processes described in this chapter do not claim any accordance with the Scytl software and are to be considered fictional.

Building The server-sided voting system including the servers and the internal network is located in a secured building of the VSP. The server computers are placed inside secured rooms. The building and the server rooms are protected against unauthorized access. To do so the VSP implements the specific safeguards from IT-Grundschutz we identified for this purpose. As before we denote them with (S x.xx) and briefly describe their implementation according to the IT-Grundschutz catalog (for details see [59]). The VSP defines entry regulations and controls in an access control concept that considers organizational and technical aspects (S 2.17). The VSP installs safety doors and windows according to the DIN EN 1627 standard that are resistant against intrusion (S 1.19, S 1.10). The VSP instructs the personnel to keep the windows and doors closed, unoccupied rooms are regularly checked for being locked (S 1.15, S 1.23). The keys are issued only to authorized personnel, their secure handling and storage are managed by corresponding rules (S 2.14). The site access authorizations are technically implemented by security locks at the building and biometric fingerprint readers at the server room entrances (S 2.6). The building and the server rooms have video surveillance systems installed in order to monitor server access and detect malicious intrusion (S 1.53).

To support the high-availability of the voting system the server rooms are equipped with a local uninterruptible power supply for bridging short-term power failures (S 1.28). For longer duration failures the components of the technical infrastructure are installed redundantly (N+1 principle) including a secondary power supply and communication links or air conditioning (S 1.56, S 1.52). To guarantee and maintain operation the VSP

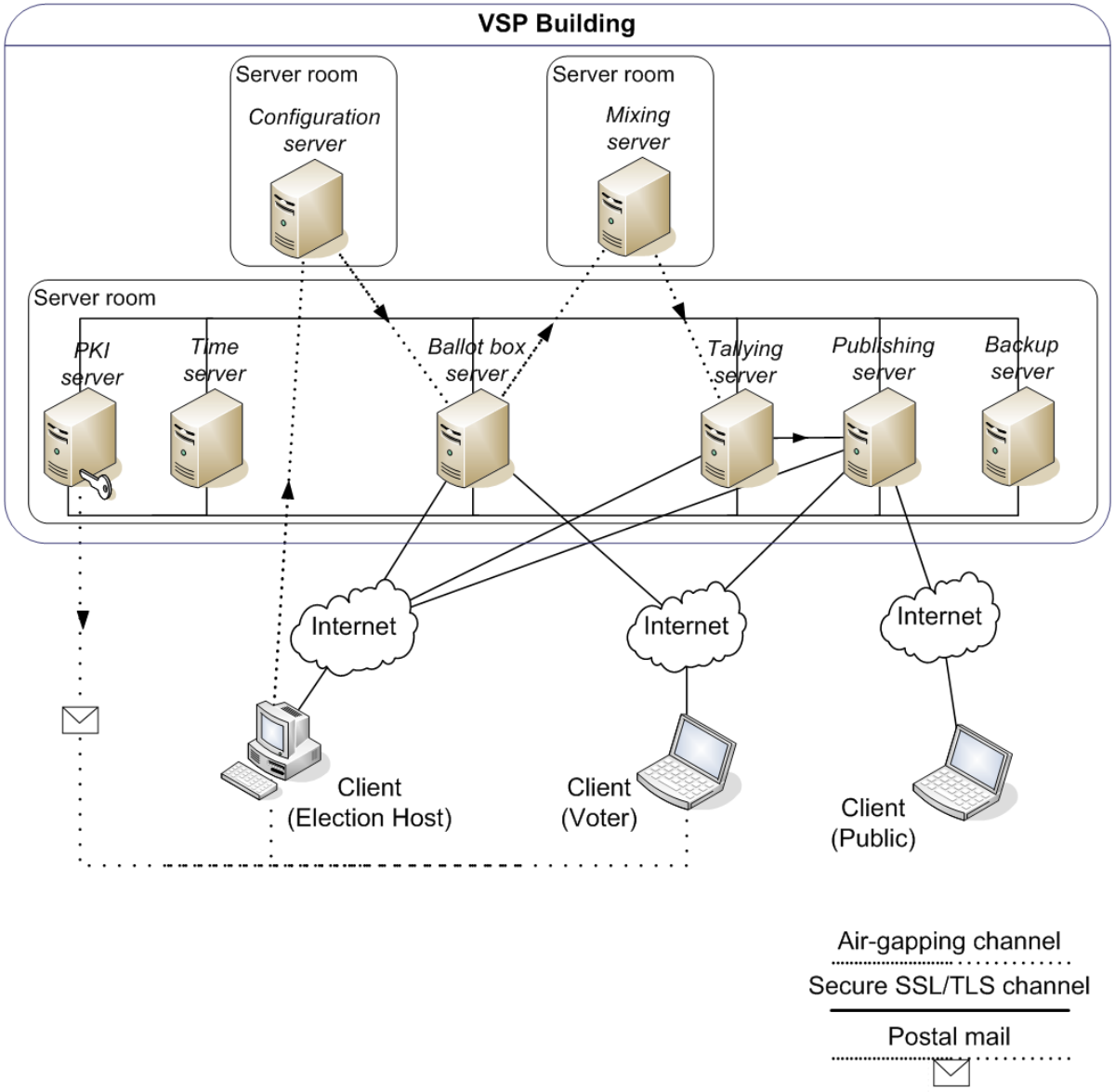

Figure 7.1.: VSP architecture

protects the server rooms against emergencies like fire and water. Patch panels that interconnect the network components are equipped with high-temperature enclosures (S 1.62). Inside the server rooms a ban on smoking is imposed and fire extinguishers are installed (S 2.21, S 1.7). Emergency circuit-breakers enable the VSP to switch of electricity in case of fire (S 1.26). Overvoltage protective measures reduce damage to the voting system components (S 1.25). Water pipes in the server rooms are avoided to prevent leakage (S 1.24). The VSP implements an alarm system that detects dangerous events like fire, water or unauthorized entrance (S 1.18) and prepares alert plans and drills (S 6.17).

Server computers While the generic VSP model used a simplified single server setup the VSP in our design proposal operates several servers for different tasks. At first we describe the servers that are required by the Scytl voting system (see [99] for details). The *configuration server* is used to process the election configuration data provided by the Election Host in order to customize the voting system according to the specific election scenario. The configuration server is isolated and disconnected from the network. The VSP uses a *Public Key Infrastructure (PKI) server* for generating and managing cryptographic keys and certificates. Concerning the cryptographic algorithms and their key length the VSP deploys up to date standards according to official recommendations following IT-Grundschutz (S 2.164) and BlueKrypt [35]. The *ballot box server* stores all incoming ballots sent by the voters. It is therefore connected to the external network to be accessible by the voters. Moreover it is accessible by the Election Host to allow him to check the ballot box before the election and to start and stop the voting phase. The *mixing server* is used for mixing and decryption of the votes after casting. It is isolated and disconnected from the network. The *tallying server* hosts the tallying application used to count the votes after mixing. It is connected to the external network in order for the Election Host to initiate the tallying process. The *publishing server* contains the final results for review by the voters, the Election Host and the public. It is therefore connected to the external network. There are two more servers that result from the IT-Grundschutz safeguards we identified in Chapter 6. As before the safeguards are labeled (S x.xx) and described according to the IT-Grundschutz catalog (see [59] for reference). The VSP operates a *time synchronization server* which provides correct time for all components and web services of the voting system. To this end the VSP implements the Network Time Protocol (NTP, specified in RFC 1305 [89]) on the server which then retrieves correct time information from external services and makes it available to the components of the voting system (S 4.227). The VSP integrates a time stamp service to obtain time stamps that are used to assign the correct time to recorded events in the election protocol (S 5.67). At last the VSP installs a *backup server* that is used to backup election data including the voting results and election protocol data (S 4.168). The backup server uses appropriate archival media according to the catalog in S 4.169 to ensure secure data storage. The backup process is implemented on a regular basis following a data backup policy (S 6.32). It includes all server-sided components of the voting system except the isolated servers for configuration and mixing and the publishing server.

In Chapter 6 we identified IT-Grundschutz safeguards to secure the server computers. Malicious collusion is prevented by logical or physical separation. The configuration server and the mixing server are isolated and disconnected from any network. They are installed on separate hardware and located in separate secured rooms (S 5.61). On all servers voting-specific software is separated logically from other installed components by means of adequate software design (S 5.62). The VSP determines the specific needs of the different servers regarding hardware and software, connectivity and security precautions based on their particular function (S 2.315). Then the servers are securely set up. The operating systems are installed and updated with current patches (S 2.318). The user, database, and network settings are correctly configured (S 4.237). The VSP determines

safeguards and procedures to protect the servers from virus infections (S 2.154). Anti-virus software is installed on all servers (S 2.156). To ensure the integrity of the servers their file system is checked regularly for any changes (S 4.93). To achieve high availability the VSP chooses computing power and storage capacity of the servers adequately to guarantee the necessary performance of the voting system. Moreover it implements redundancy strategies including a secondary system that can be switched over to in case of failure of the primary system (S 2.314). Therefore all servers are provided twice with identical configuration (to reduce complexity of the architecture overview we illustrate each server only once in Figure 7.1). The VSP prepares a contingency plan for the operation of the servers in order to minimize the effects of server failures (S 6.96).

Those servers connected to the external network act as web servers. For their secure operation we identified the following IT-Grundschutz safeguards in the last chapter. The VSP sets up the web servers regarding at least access restrictions, interoperability and data accessibility (S 2.175). Following S 2.220 the VSP implements access controls based on assigning role-based permissions. Authorized access to the servers by VSP personnel is granted based on authentication using smart cards (S 2.7). The VSP ensures that publicly accessible data is protected against subsequent change by means of digital signatures (S 4.99). To facilitate the management and processing of election data the servers have database systems installed. The databases are included in the regular data backup with the exception of the isolated servers and the publishing server (S 6.49). The database integrity is ensured by implementing comprehensive control functions (S 2.130). In case of any problems additional procedures are defined to restore the databases to a stable condition based on backups (S 6.48).

Internal Network The internal network interconnects the server-sided components of the VSP. The encryption of the network traffic is achieved using adequate mechanisms as proposed by the identified IT-Grundschutz safeguards (e.g. IPsec or SSL) (S 5.66, S 5.68). However the voting system at hand requires a special connection type for specific components (see [99]). For the purpose of higher security, the VSP connects configuration server, ballot box server, mixing server and tallying server using air-gapping channels. To minimize the risk of interference, the VSP disconnects these servers from any network as far as possible (while the configuration server and the mixing server are completely isolated, the ballot box server and the tallying server are connected to the external network for the limited time frame when they need to be accessed by the voters or the Election Host). Data are transferred using an air-gapping approach. To this end, information is securely stored on removable media (e.g. memory sticks or burned DVDs) and transferred to the server by authorized and instructed personnel of the VSP.

To make the voting system accessible for the outside actors a security gateway is used. It includes a firewall, routers and switches to couple the internal network with the Internet. The VSP configures all network components securely following a predefined network concept. Here we use again the previously identified safeguards from IT-Grundschutz. The network concept includes the handling of network protocols and ports to manage access rights, implementing filter rules to control communication flow as well as

using passwords and checksums to ensure that routing tables and network configuration data cannot be tampered with (S 4.82). The gateway represents the interface between the voters and the voting system. Hence its availability is of crucial importance. Therefore the VSP installs all gateway components redundantly (S 6.53, S 2.302). Moreover it implements contingency procedures to maintain the availability of the gateway components even during emergencies (S 6.94, S 6.92). The gateway is protected against network attacks like DNS spoofing and is able to detect and respond to unauthorized intrusion attempts (S 5.59, S 5.71). This helps preventing insecure network access. It is additionally supported by regulating and controlling all internal data transmissions (S 2.204). Following the VSP's general guideline to restrict access based on roles, the access to network components for authorized VSP personnel is regulated using passwords and smart cards as authentication tokens (S 2.220, S 2.7). The configuration data of all network components are included in the regular data backup plan in order to be recoverable (S 6.52, S 6.91).

Secure Communication Channels The secure communication channels connect the VSP with the external actors (Election Host, voters, public). These connections are routed through the Internet. The SSL protocol ensures integrity and confidentiality of the communication data as described in the identified IT-Grundschutz safeguards (S 5.66, S 5.68). It is supported by most standard software (browsers etc.). This facilitates usage on the client side. Critical authentication data (in the scenario at hand these are the certificates of the Election Host and the passwords of the voters) are delivered using postal mail instead of electronic channels to prevent eavesdropping or similar network attacks. In order to transfer election configuration data to the configuration server, the Election Host uses an air-gapping channel (see previous paragraph). For the delivery of authentication means and key material to the voters and the Election Host, the VSP uses secure postal mail, namely registered letters in sealed envelopes.

Software Following the Austrian election scenario we use the Pnyx.Core voting software from Scytl as the technical basis[5] [40, 99]. It is an online voting scheme based on cryptographic mechanisms. Pnyx.Core aims for scalability, provides auditing capability and multiple voting channels (web browsers, mobile phones etc.), and does not require client-side installation[6]. This suits the VSP scenario. It has been used successfully in many elections[7]. For configuration purposes, the additional Scytl Pnyx Election Configuration module is used [100]. As described in IT-Grundschutz safeguard S 2.8, authorized access to the software systems is based on a "need-to-know principle" to limit the access rights to the minimum required for the particular tasks. This is implemented by defining corresponding read and write permissions for accessing applications and data. The voting software code is digitally signed to ensure its integrity.

Remark. Our results in Chapter 6 revealed that voting software certified according to

[5] See remark on page 78.

[6] `http://www.scytl.com/en/pnyx-core-p-4.html`

[7] `http://www.scytl.com/en/customers-c-10.html`

the Protection Profile (PP) for online voting products [64] is able to satisfy the majority of technical requirements for the voting software that we identified in Chapter 5. At the current moment, there is no publicly documented voting software available that is certified for compliance with the PP. Therefore we cannot provide a corresponding description in this design proposal. Instead, we use the Pnyx.Core software being an approved and commonly used online voting protocol that allows us to specify the VSP architecture and processes and then concentrate on the implementation of the operational environment. We point out that in order to follow our recommendations to satisfy the corresponding technical requirements for VSPs a PP-certified voting software is supposed to be used.

Client devices The client devices are used by the voters, the Election Host and the public to exchange data with the VSP. The clients must have Internet access to establish a network connection to the VSP. They must meet the minimum requirements as required by the voting software. In particular they must support SSL for a secure Internet connection (S 5.66) and have the Java Runtime Environment installed (cf. [31, p. 057]). In the scenario under analysis the vote-casting devices are standard home PCs or kiosk systems with Internet access. The VSP provides public information on minimum requirements and configuration to assist the voters in handling their devices.

7.4. Processes

We specify the processes of the VSP during the pre-voting, voting and post-voting phases. Therefore we describe the single processes in detail and note the involved actors and components from the VSP architecture. While the processes are based on our generic VSP model, most of them are adapted or expanded due to the Scytl voting system. Therefore the detailed descriptions follow the specifics of the voting system as given in [99]. As before we further refine the generic model by incorporating the IT-Grundschutz safeguards we identified in Chapter 6 and describe their implementation briefly according to the IT-Grundschutz catalog (see [59] for a full description). The safeguards are denoted by their numbers (S x.xx). Each voting phase is visualized using an Unified Modeling Language (UML) use-case diagram to illustrate the functional relations between the involved actors [71]. The workflows and interactions are summarized in an UML sequence diagram.

7.4.1. Pre-voting phase

The processes of the pre-voting phase are displayed in Figure 7.2. The interactions are illustrated in Figure 7.3.

Registration

Actors: VSP, Election Host

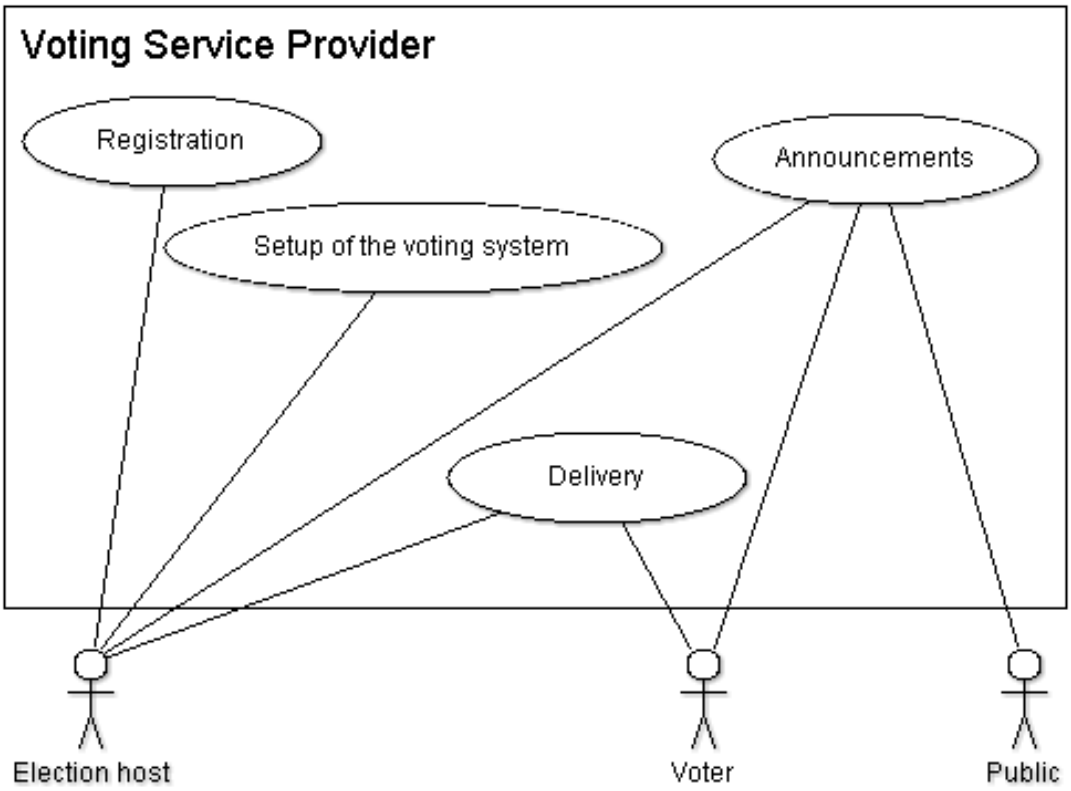

Figure 7.2.: Pre-voting phase

Architecture: Secure communication channels, PKI

The Election Host, in more detail the electoral board, identifies the eligible voters and generates the electoral roll information. In the analyzed scenario all Austrian students were eligible and therefore no active role in the registration was necessary. Using a secure communication channel, the Election Host transmits the information to the VSP which prepares the data for use in the voting system. More precisely it augments the electoral roll information with corresponding PKI data (see paragraph "Setup of the voting system").

Delivery

Actors: VSP, Voters, Election Host

Architecture: Secure communication channels

The VSP securely delivers passwords to the voters, digital certificates to the Election Host and the shares of the private election decryption key to the members of the electoral board (see [99] for details on these credentials). For this purpose we take the following identified safeguards from IT-Grundschutz: the VSP uses registered letters in sealed envelopes to ensure correct and personal delivery (S 5.23, S 2.44). The personnel is

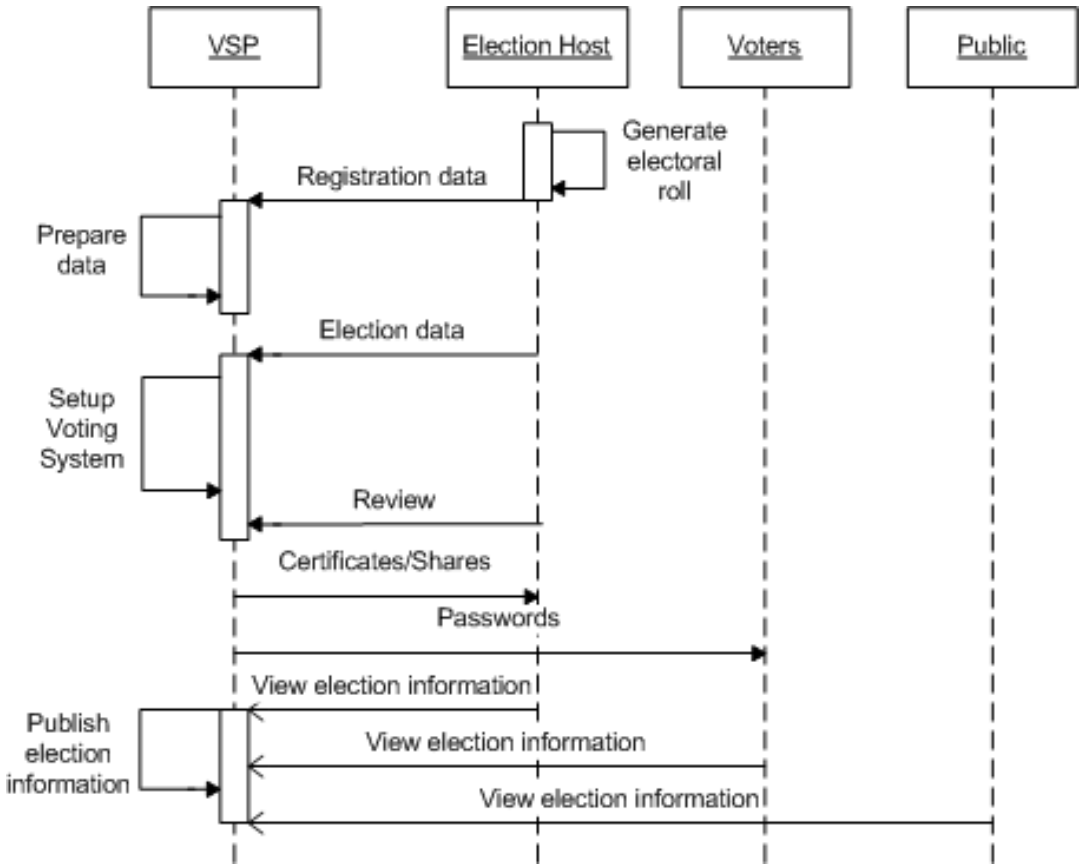

Figure 7.3.: Pre-voting phase interactions

briefed on secure delivery procedures, the letters are checked for correctness and do not reveal unnecessary data (S 3.14, S 2.45).

Announcements

Actors: VSP, Voters, Election Host, Public

Architecture: Publishing server

The Election Host transmits the candidate list and the election time table including starting and ending time of the voting phase to the VSP which publishes the information on his Internet portal accessible by the Election Host, the voters and the public. The VSP assigns the necessary access rights for the particular tasks (S 2.8).

Setup of the voting system

Actors: VSP, Election Host

Architecture: Configuration server, Internal network, PKI

The VSP uses digital signatures for identification and authentication of the eligible voters and the Election Host. Therefore the PKI server issues the required cryptographic keys and digital certificates before the election. Appropriate algorithms for digital signature based authentication techniques are chosen following the recommendations given in safeguard S 2.164 and at BlueKrypt [35]. The generated authentication data is protected by means of password policies and encryption (S 4.133). The VSP securely stores the private keys of the voters in the ballot box server protected by passwords.

The databases on the servers are prepared so that all parameters suit the current voting scenario's needs regarding table size and user access rights management (S 2.125). The Election Host is registered at the voting system, and the members of the electoral board provide the necessary election data (electoral roll, election scheduling data etc.). The VSP adds the authentication data to the electoral roll for all eligible voters. In consultation with the Election Host the VSP sets the electronic ballot representation. Finally the VSP enables the Election Host to review the election configuration information including the "unique election identifier" (as used by the Pnyx.core voting system, see [99]), election time schedule, electoral roll as well as opening and closing tokens which specify start and end of the voting phase. The VSP assists the Election Host via his help desk (see paragraph "Help desk", S 2.12). The data then are digitally signed by the Election Host and transferred to the isolated configuration server using an air-gapping channel. There the data are included in the corresponding database. The VSP takes care of completeness, format compatibility and integrity (S 2.135). Then the voting software is configured using Scytl's Pnyx Election Configuration module [100].

Next the VSP checks that the database on the ballot box server is empty. If not, old data is erased securely using fileshredding software which overwrites electronic data randomly thereby making recovery impossible (S 2.167). The Election Host is enabled to witness this procedure. The VSP uses its PKI to generate the private election decryption key. The key then is split into shares following a secret-sharing approach as required by the voting system (see [99]). The original key is securely erased (S 2.167). The VSP stores the shares on smart cards and securely delivers them to the members of the electoral board using postal service (see paragraph "Delivery").

7.4.2. Voting phase

The voting phase is visualized in Figure 7.4. The interactions are illustrated in Figure 7.5.

Opening the election

Actors: VSP, Election Host

Architecture: Secure communication channels, Ballot box server, Client device (Election Host)

The Election Host establishes a secure communication channel to the VSP and initializes the voting phase by certifying the opening token (cf. [99]). The VSP then installs

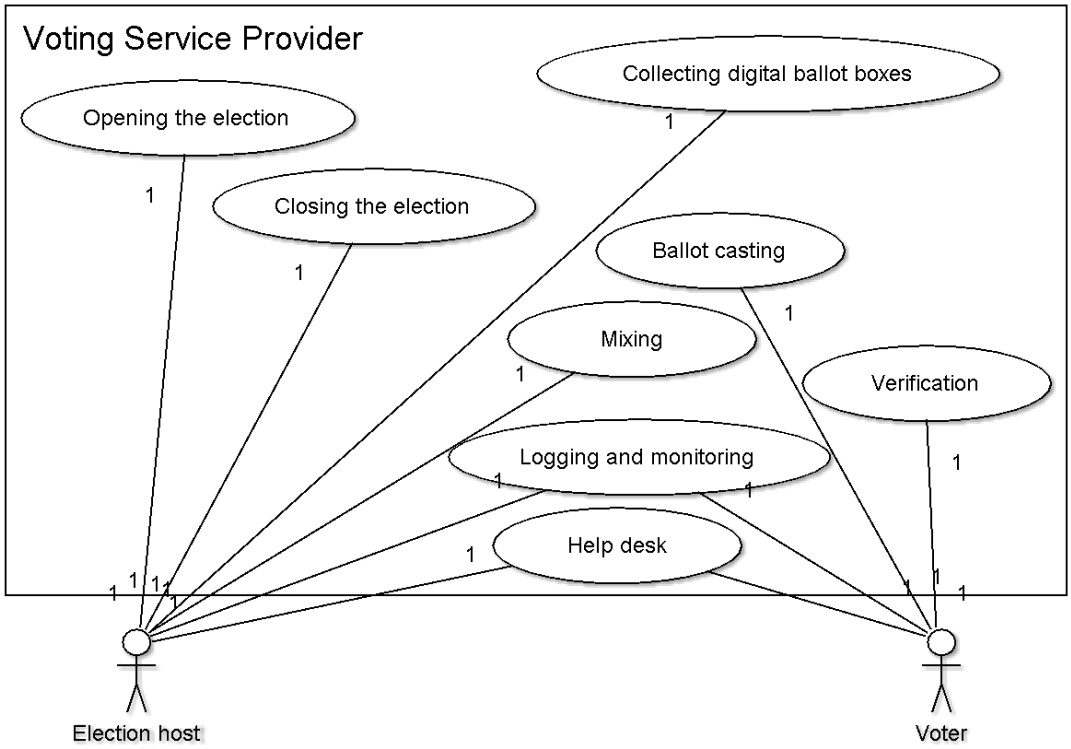

Figure 7.4.: Voting phase

it in the ballot box servers in order to start the ballot casting. The VSP assists the Election Host on doing so (see paragraph "Help desk", S 2.12).

Ballot casting

Actors: VSP, Voters

Architecture: Secure communication channels, Ballot box server, Client device (voter), PKI

The VSP provides a secure communication channel between the ballot box server and the client device of the voter. The voter receives the voting options layout from the ballot box server and fills out the ballot. The VSP provides a digitally signed applet that the voter uses to verify his selected voting options. Then the ballot is encrypted using the public key of the Election Host (S 4.34). It corresponds to the shared private key used to decrypt the votes. The client applet generates a "receipt signing request" (as used by the Pnyx.core voting system, cf. [99]) signed by the voter's private key (see paragraph "Setup of the voting system"). The voter enters the password and downloads the private key from the ballot box server. The voter sends the encrypted ballot and the receipt signing request to the VSP's ballot box server. The ballot box server verifies the signature of the receipt signing request and checks the voter's eligibility. The encrypted vote and the receipt signing request are stored in the digital ballot box. The ballot box

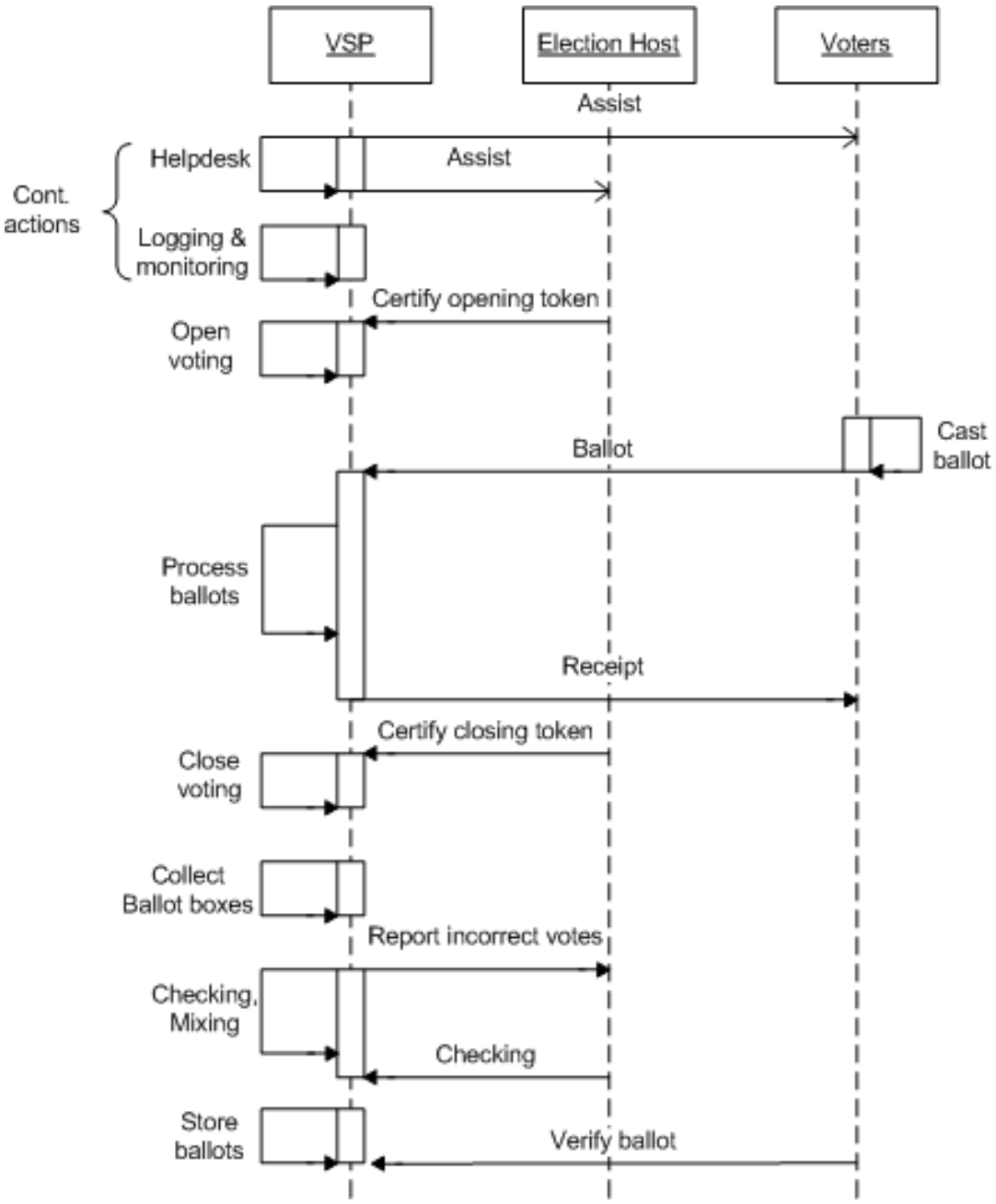

Figure 7.5.: Voting phase interactions

server sends an electronic receipt to the voter by means of a digital signature. At the end of the ballot casting process the ballot box server digitally signs the ballot boxes (S 4.34).

Closing the election

Actors: VSP, Election Host

Architecture: Secure communication channels, Ballot box server, Client device (Election Host)

Following the Scytl Pnyx.core voting system functionality, the Election Host establishes a secure communication channel to the VSP and terminates the voting phase by certifying the closing token. The VSP then installs the token in the ballot box server in order to stop the acceptance of new ballots. The Election Host defines a timeout period in which voters can finish casting their votes. The VSP assists the Election Host on doing so (see paragraph "Help desk", S 2.12).

Collecting digital ballot boxes

Actors: VSP, Election Host

Architecture: Ballot box server, Mixing server, Internal network

This process results from the specific procedures of the Scytl Pnyx.core voting system (cf. [99]). The VSP collects the digital ballot boxes in order to prepare them for mixing the contained ballots. Then the VSP transfers the ballot boxes to the mixing server using an air-gapping channel. The VSP enables authorized members of the Election Host to witness these steps.

Mixing

Actors: VSP, Election Host

Architecture: Ballot box server, Mixing server, Tallying server, Internal network

As before this process results from the specifics of the Scytl voting system. It uses a mixing approach to anonymize the votes [99]. The VSP checks authenticity and integrity of the ballot boxes and ballots by verifying the digital signatures (S 4.34). The eligibility of the voters is checked by verifying the digitally signed receipt signing request. The VSP reports incorrect votes to the Election Host and separates them. The electoral board members jointly reconstruct the decryption key by contributing their shares. The VSP detaches the digital signatures from the valid ballots. Then the ballots are mixed using a verifiable mix-net which allows the VSP and the Election Host to verify the correctness of the mixing process. Then the VSP decrypts the votes and stores them securely while it erases them securely from the mixing server's memory using fileshredding mechanisms (S 2.167). Next the VSP shuffles the receipt identifiers which were detached from the votes before mixing. It stores the receipt identifiers securely and separates them from the stored votes. Then the Election Host uses the private election key to digitally sign the list of decrypted votes and the list of receipt identifiers. The VSP again takes care of secure erasure of the private decryption key of the Election Host. At last the VSP transfers the list of decrypted votes and the list of receipt identifiers to the tallying server using an air-gapping channel.

Verification

Actors: VSP, Voters

Architecture: Publishing server, Client device (voter), Secure communication channels

The VSP enables the voters to verify the published election results. The voting system allows the voters to verify that their ballots indeed reached the proper electoral authority and were included in the final tally. To perform the verification the voters need to verify that their unique receipt identifier (generated during ballot casting) is included in the ballot verifiability list (generated during mixing). Therefore the voter downloads the information from the VSP's publishing server using a secure communication channel. The VSP provides assistance to the voters how to perform the verification and how to issue public objection in case of failed verification (see paragraph "Help desk", S 2.12).

Logging and monitoring

Actors: VSP, Election Host, Voters

Architecture: Building, Server computers, Internal network, PKI

According to the law the VSP is required to record all essential data, events and actions of the election in an election protocol. For this purpose we identified several IT-Grundschutz safeguards in Chapter 6. The VSP continuously monitors all system components and processes relevant for the election. The server computers record corresponding log files which are reviewed by the VSP at regular intervals (S 5.9). Regarding the databases on the servers the VSP monitors the access statistics, the number of database connections as well as data modifications and failures of data storage (S 2.133). The available space and the fragmentation of the databases are monitored to prevent systemic failure (S 4.70). The VSP also monitors its internal network infrastructure. All network components are regularly checked for their system performance and correct operation in order to detect network problems, failures or even intrusions (S 4.81). The rooms' entrances and the servers within are monitored throughout the election period using video surveillance system (S 1.53). The system configuration and operation as well as changes made to the voting system are documented. All data from these log files are included in the election protocol. The system uses cryptographic mechanisms like digital signatures and hash functions to preserve integrity, authenticity and non-repudiation of the recorded information (S 4.34). Necessary key material is issued by the VSP's PKI. The VSP assists the Election Host to supervise all relevant election processes (see paragraph "Help desk", S 2.12). All configuration data and critical operation can be reviewed and controlled by the Election Host.

Help desk

Actors: VSP, Election Host, Voters

Architecture: Secure communication channels

In accordance with our results from Chapter 6 the VSP provides assistance to the voters and the Election Host on all questions concerning the election, the voting system and related technological security issues. The help desk can be contacted via email and phone throughout the election period (S 2.12). It is made known on the VSP's Internet portal to all users (S 3.46). The help desk is also concerned with the briefing of voters and the Election Host. Therefore the VSP provides user guidelines on a special website of the Internet portal that can be accessed via secure communication channels. The instructions consider all important procedures and the secure handling of the voting system and the client devices in accordance with the law (S 3.1, S 3.4, S 3.26). Besides election specific briefing the voters and the Election Host are advised on general IT security issues to avoid problems that result from incorrect usage or behavior, for example procedures in case of computer virus infections or to prevent social engineering attacks (S 2.198, S 3.5).

7.4.3. Post-voting phase

The post-voting phase is visualized in Figure 7.6. The interactions are illustrated in Figure 7.7.

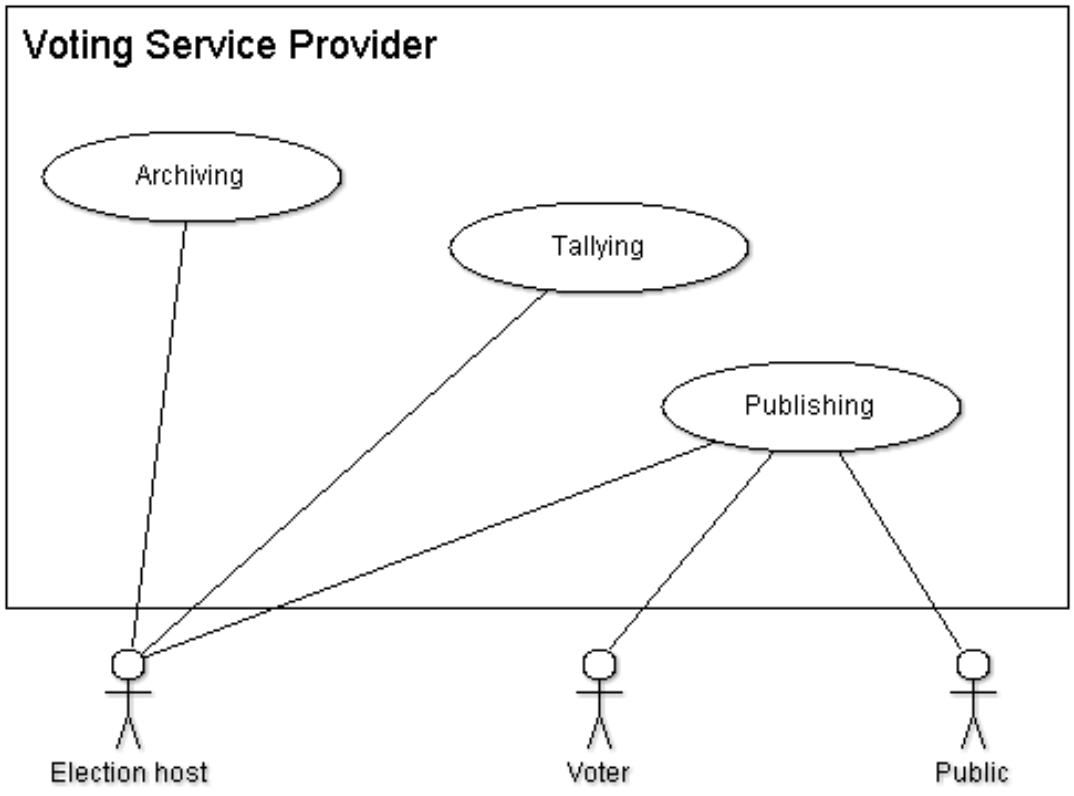

Figure 7.6.: Post-voting phase

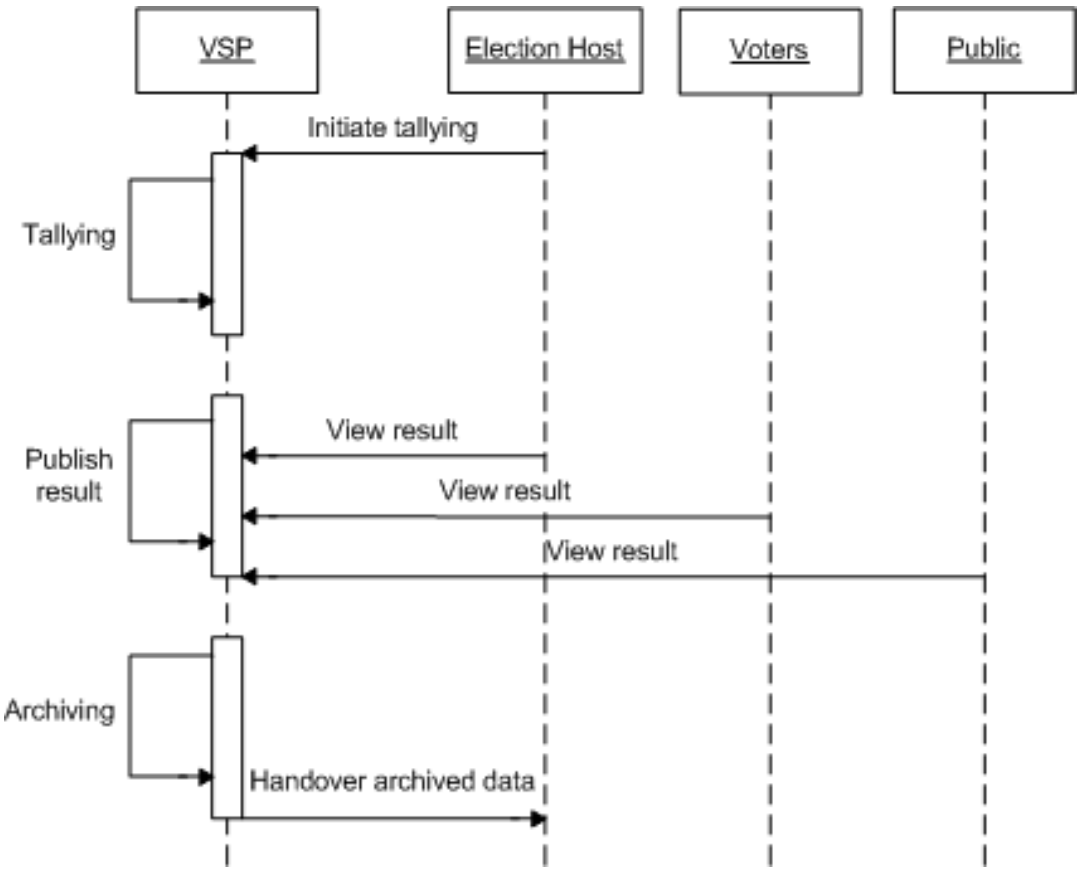

Figure 7.7.: Post-Voting phase interactions

Tallying

Actors: VSP, Election Host

Architecture: Tallying server, Client device (Election Host), Secure communication channels

Using a secure communication channel to the VSP's Internet portal, the Election Host authenticates at the tallying server. Then the Election Host initiates the tallying process which is securely operated by the VSP on the tallying server. The VSP enables the Election Host to monitor and review the tallying process. It assists the Election Host on performing these steps (see paragraph "Help desk", S 2.12).

Publishing

Actors: VSP, Election Host, Voters, Public

Architecture: Publishing server, Client device (all), Secure communication channels

The VSP publishes the final result and the verification list on the publishing server where the data can be accessed by the voters, the Election Host and the public via their client devices using a secure communication channel.

Archiving

Actors: VSP, Election Host

Architecture: Backup server

This process expands the generic VSP model as a result from the previously identified safeguards. In most election scenarios respective legal regulation prescribes that specific election data has to be archived for a certain time period. The VSP determines the specific archiving objectives for the election scenario at hand and therefore considers the legal demands (S 2.242, S 2.245). It securely stores the decrypted votes for later recount using the backup server. Moreover it stores the election protocol which results from the logging and monitoring process for later review of the correct election operation. In accordance with the law (Austrian Students Association Ordinance, [20]), the VSP hands over the archived election data on secure storage media to the Election Host where it is archived for five years.

8. Discussion

In this chapter we review the Voting Service Provider (VSP) concept and discuss some open issues. This chapter is based on work we published in [P4].

8.1. Review of the VSP Concept

As stated in the introduction of this thesis, an important motivation for the VSP concept is the proposition that the secure implementation of online elections implies high efforts and costs. Now we want to review the results of our work in this respect. In this thesis we identified the requirements for secure online elections. To this end we used legal as well as technical sources. The legal regulation for VSPs considers the applicable law in Germany (see Chapter 4). The technical sources we used to concretize and extend the legal requirements are up-to-date and comprehensive since our main source, Volkamer's list of requirements [109], is based on an extensive analysis of the recent literature on requirements for electronic voting, including for example the approved recommendations on "Legal, Operational and Technical Standards for E-voting" from the Council of Europe [48], or the requirements catalog "Online-Voting Systems for Non-parliamentary Elections" developed by the German National Metrology Institute [75]. The former has been considered in several e-voting implementations, like for example in Switzerland (see [21, p. 20] and [37]), or in Austria (see [82, p. 39]). Hence we consider the resulting list of technical requirements well-founded (see Chapter 5). As a first result this proves that even in a non-political election scenario as considered in this thesis there are indeed many requirements that have to be satisfied in order to realize secure online elections. In Chapter 6 we have demonstrated that even voting software certified according to the current Common Criteria Protection Profile (PP) for online voting products [64] cannot fulfill these requirements alone. Instead, the results reveal that there are many requirements that have to be satisfied by the operational environment. They include structural aspects like a secure building or server rooms, technical aspects like secure network connections and a highly available voting system, as well as organizational aspects like the secure configuration of the voting system and qualified personnel. Our results further demonstrate that there are many complex safeguards that have to be implemented in order to satisfy these requirements. To name a few examples, secure communication channels have to established, backup and redundancy systems need to be implemented, emergency concepts for protection against fire, water or power failure must be developed, the personnel must be trained and instructed and a help desk needs to be provided. Moreover in order to ensure the secure and trustworthy implementation of all safeguards an evaluation and certification procedure should be performed. This

implies additional efforts and costs. Based on our results we therefore conclude that the initially made proposition is correct – the implementation of secure online elections indeed requires high efforts and costs. If a VSP is used all this needs to be done only once for many elections while the Election Hosts are relieved of these issues. In addition, using a VSP reduces the necessary tasks for the Election Hosts during the election, as becomes apparent in the process diagrams in the design proposal in Chapter 7. Altogether this supports the idea that the VSP concept makes online elections more practicable. Still, for a scientifically founded statement regarding the practicability the economical aspects of the VSP concept would have to be researched in detail.

8.2. Certified Trustworthiness vs. Verifiable Protocols

The VSP concept involves the evaluation and certification of the VSP's software and operational environment to ensure election security and legal conformance. In Chapter 1 we introduced the idea of verifiable voting protocols as an alternative approach to strengthen election security at the software level. Now we review this idea in the light of the results of the thesis. As mentioned before, Schneider found that not all classes of security properties can be enforced by software techniques like execution monitoring. Our results support this finding. In Chapters 5 and 6 we identified many requirements for secure online elections that involve procedural support in the operational environment. For example, integrity requires the accurate transfer of the election data into the voting system (Technical Requirement 9), authentication mechanisms that enforce eligibility and only one vote per voter (Technical Requirement 7), or the secure setup of the voting system (Technical Requirement 11). To ensure the availability of the voting system, redundant components and an emergency service are necessary (Technical Requirement 3 and 5). To ensure the confidentiality of election data, access protection is required even at the physical level (Technical Requirement 6). Moreover, procedural measures enable controlling the election stages (Technical Requirement 10), or a help desk for voters (Technical Requirement 19). This confirms the necessity of a secure operational environment that can be realized by a VSP. Nevertheless, the VSP concept can benefit from verifiable voting protocols. To bring these two approaches together, a VSP could use a powerful protocol that guarantees certain security properties. Thereby the VSP does not need to address these properties in its operational environment which reduces efforts and costs. Moreover, as we pointed out in Chapter 4.4.3, verifiable protocols are often complex and thereby involve configuration and usability issues. This requires advanced skills and knowledge of both the election operator and the voters. However, this can easily be addressed by a VSP that employs qualified personnel to set up the voting system correctly and provides a help desk for the voters (Technical Requirement 1 and 19). In this way, the VSP concept can facilitate the use of verifiable protocols in practice. Moreover it allows evaluating and certifying not only the protocol but architecture, components and processes to ensure the security of both the protocol and the operational environment.

8.3. Centralized VSP vs. Distributed Approaches

The VSP concept is a centralized approach. That is, the majority of security relevant components is gathered in one place under one responsibility. In the recent years, the discussion of IT security with regard to networked environments and services brought up another approach based on distributed services (see [47] for a general introduction). While having the same goal of providing secure services, some aspects of the approaches are almost opposing. We therefore want to briefly compare these two approaches and assess their respective properties.

As the majority of security critical tasks is allocated to the VSP, the idea of a single point of failure might be induced. The fact that all relevant systems are under control of one operator might raise suspicion of data abuse or deception. This is a typical security issue of centralized systems. In contrast, in distributed approaches the responsibility for critical tasks and data processing is shared among several entities. The intention is to ensure that no single entity has complete access to all systems and data which reduces the risk of misuse. Thereby the security level might be increased. Moreover the robustness can be improved because in distributed systems, security incidents like attacks or system crashes mostly affect only single parts of the system. Several security techniques have been introduced in the field of electronic voting that are based on that idea: distributed mix-nets intend to anonymize votes, no single involved server can read the votes (see [46]). Secret sharing mechanisms ensure that recovering a secret information requires a group of entities to work together, often used for distributed decryption of votes (see [101]). Mostly this idea is applied as a threshold encryption scheme, where only a subset of entities is needed to decrypt the information in order to ensure robustness of the system even if certain entities are malicious. Several schemes assume multiple authorities which jointly decrypt the votes. These techniques are used in many electronic voting protocols, e.g. the schemes of Juels et al. [79], Baudron et al. [34], Lee and Kim [86], or the Helios scheme of Adida [27, 28]. However, distributed systems imply some difficulties. Trust in distributed systems is based on the assumption that it is most unlikely that all entities are malicious. While a subset of malicious entities cannot affect the system security it is still necessary that the majority of entities behaves correctly. However, this can hardly be guaranteed since distributed systems are much more difficult to supervise. Moreover, the large number of entities requires a sophisticated communication network and comprehensive coordination. Therefore additional measures are required. This increases complexity of such systems and can possibly endanger their reliability.

In contrast, centralized systems simplify regulation, evaluation and supervision. In a distributed system, ensuring the observation of legal provisions and security requirements is difficult because control and auditing mechanisms would have to be installed at many locations. This complicates guaranteeing legal compliance. In centralized systems, requirements for communication and coordination are reduced and compatibility among system components can easily be ensured. This reduces complexity and improves reliability and robustness. We argue that the problem of a single point of failure can be significantly reduced by first a legal regulation that stipulates comprehensive security

requirements, secondly an accreditation procedure that verifies the implementation of corresponding safeguards by means of evaluation and certification, and thirdly the continuous supervision of operation by a Supervisory Body. The advantages of a centralized service provider have proven themselves in the analogical concept of a Certification Authority (CA). We conclude that both approaches have advantages and disadvantages. The basic intention of this thesis is to introduce the concept of outsourcing to electronic voting in order to provide a practicable approach to enable secure online elections. The proposed VSP concept demonstrates that this idea can be realized. Thus we consider the centralized concept a simple and promising approach.

The discussion on centralized and distributed approaches also raises issues regarding the technical implementation of anonymization techniques. In the following we consider the question whether mix-nets or homomorphic encryption schemes are more suitable for VSPs. Today's electronic voting protocols mostly use mix-nets [46] or homomorphic encryption [76] in order to ensure the anonymity of votes. For example, the Scytl Pnyx.core voting system [99] which was used in the design proposal is based on a mix-net (see Chapter 7). Another example is the protocol of Juels, Catalano and Jakobsson [79]. A typical example for a protocol based on homomorphic encryption is Helios 2.0 [28]. Basically one might argue that the security benefit of mix-nets is based on their distributed operation. This cannot be provided by the centralized VSP concept. Homomorphic encryption techniques could be used instead in order to realize anonymization of votes. Here a distributed network is not required. Individual votes are never decrypted and thus it is impossible to link a vote to its voter. Only the summarized result of all votes is decrypted. This could also improve efficiency of the system. On the other hand, homomorphic schemes have several limitations. In general, ballots can only be represented in a numeric format. Hence, not all types of ballot templates can be used in the electronic election [78, 96, 41]. Moreover most homomorphic schemes involve Zero-Knowledge Proofs to prove the correctness of votes [41]. This increases computational complexity of the scheme for complex ballots while reducing usability for the voter. Moreover it involves implementation issues in specific election types like preferential voting [85, 96, 98, 29]. Furthermore, many homomorphic schemes encounter scalability issues due to the fact that decryption involves solving discrete logarithms. Here the complexity increases with the number of votes, hence efficiency is at stake for large elections [49, 41, 78].

Since the VSP is intended to operate any kind of election in many different election scenarios it is preferable to deploy a more flexible system to be able to adapt to the particular requirements of the different election scenarios. In general, mix-net based schemes provide better flexibility and scalability [41]. From this perspective, a mix-net seems more suitable for VSPs. One might argue that a single-node mix-net like in the VSP's case could compromise the anonymity of the votes if this server is malicious. But the same holds for homomorphic schemes. In both cases the server has to be isolated and kept under surveillance. On the other hand, a single-node mix-net improves efficiency. Distributed multiple-node mix-nets only make sense if the particular nodes are operated by parties of different interest. This might complicate implementation in practice. And still, in order to prevent global collusion, multiple-node mix-nets also have

to be isolated and monitored. Since the VSP concept allows for easy evaluation of the system and moreover provides a highly secure operational environment including protection and surveillance measures, such single-node mix-nets can be operated securely. To sum up, both approaches could be operated securely by a VSP and therefore utilized dependent on the election scenario and the preferable properties. Homomorphic schemes are possibly easier to integrate in the VSP scenario, mix-nets provide more flexibility and scalability which is considered desirable for the VSP scenario.

9. Future Work and Conclusion

We consider some open questions and future work. In Chapter 4 we discussed the applicability of the legal regulation for Voting Service Providers (VSPs) to political election scenarios. Based on the judgment of the German Constitutional Court we concluded that to this end, specific requirements for voter-verifiability and usability have to be satisfied. Finding appropriate solutions is an important challenge for the scientific community. We argue that a combined approach of a sophisticated voting protocol and supporting external measures like evaluation and certification, optimized user interfaces, and voter assistance are a promising starting point. Since its functionality and operation can be regulated and certified the VSP could be made responsible for implementing such measures. By correspondingly extending the legal regulation even political elections with VSPs could be made possible. Currently there exists no approved solution to these problems. It is therefore an open question how exactly the VSP could contribute. Another interesting issue is whether specific voting protocols are particularly suitable for the VSP. While we argue that a VSP is able to operate a multitude of voting protocols it might be possible that certain protocol properties either facilitate or, on the contrary, complicate a secure operation in a VSP environment. This could be revealed by further studies. Next, it seems important to study the economical aspects of the VSP concept. Building a VSP from the ground up might be costly. The business profits of performing many elections may outweigh this initial investment. Moreover it is most likely that the VSP business will be performed by IT service providers with already existing infrastructure and safeguards which would reduce the investment. Still, an economic study should be performed to assess the business potential of the VSP concept.

Finally, we conclude our work. This thesis was motivated by the question how to enable secure online elections. We will now summarize our work and review the results in this respect. We introduced the VSP as a new concept that outsources the implementation of online elections to a qualified and professional third party. Then we developed an approach to make online elections with VSPs secure. As the basic security definition we presented the first legal regulation for VSPs in non-political election scenarios in Germany. This enables even legally binding online elections. Then we made the legal requirements technically usable by deriving corresponding requirements for the online voting software and the operational environment. To verify the VSP's security, we developed a practical approach to evaluate and certify the observance of these requirements. Thereby we expanded the existing approach of pure voting software evaluation [64] by incorporating the operational environment. Our approach is realistic and efficient since it allows the incorporation of existing Common Criteria and IT-Grundschutz certificates to reduce evaluation efforts and costs. The method is adjustable to higher security re-

quirements to address for example other election scenarios. A subsequent accreditation procedure officially confirms the security and the legal compliance of the VSP. This makes the VSP trustworthy. At last, we proposed how to realize a VSP in practice. This demonstrates that the VSP concept is feasible and makes secure outsourcing of online elections possible. We conclude that secure online elections can be enabled by VSPs.

A. Appendix

A.1. Abbreviations

CA Certification Authority

EAL Evaluation Assurance Level
(Evaluation level in the Common Criteria methodology)

KORA Konkretisierung Rechtlicher Anforderungen
(engl.: Concretization of legal requirements)

PKI Public Key Infrastructure

PP Protection Profile
(The basic document in the Common Criteria evaluation procedure)

UML Unified Modeling Language

VSP Voting Service Provider

A.2. Election Principles

In order to match legal and technical requirements in Chapters 4 and 5 we use the affected election principles. The definition of these principles slightly varies in the literature. We use the definition given in Volkamer [109, Chapter 4.2]. In the following we quote verbatim but omit special text formatting like bold or italic font because it has no relevance for this thesis.

Secret: [se] The voting system shall prevent anyone without the appropriate authority[1] from deducing or proving the link between a particular ·elector· and his ·vote·.

Free: [fr] The voting system shall protect the ·voter's· right to express his ·vote· in a free manner, without any coercion or undue influence.

Equal: [eq] The voting system shall ensure that each ·voter· may only ·cast· one ·vote· per ·poll·[2].

[1] In most constituencies, no such authority exists; the U.K. is one notable exception.

[2] 7 In certain ·polls·, some ·voters· may have the right to ·cast· more ·votes· than others (for example, stock corporations). Such ·polls· are not taken into account for this thesis. (A/N: This refers to the thesis of Volkamer [109])

Universal: [un] The voting system shall protect the right of an ·eligible voter· to ·cast· his ·vote·.

Direct: [di] The voting system shall determine the results of a ·poll· based on all ·votes· ·cast· and only based on these ·votes·.

Volkamer describes two more principles "in order to be able to link each requirement to at least one category" [109, p. 62]. We add these principles analogously:

Trust: [tr] The objective is to implement an electronic voting system with the aim of maximizing public trust.

Data Protection: [dp] Data protection is necessary when referring to remote electronic voting because information about the voters are used to identify him in the remote electronic voting system.

A.3. Technical Documentation

Here we cite the requirements for remote electronic elections from Volkamer [109, Chapter 6] that we use in the refinement process in Chapter 5. The requirements are listed in the order of appearance in Chapter 5. The following text is quoted verbatim. However formatting like bold or italic font used by Volkamer has been omitted because it has no further relevance in this thesis.

Op.6 [all] The ·responsible election authority· shall educate ·poll workers· in the use of the ·electronic voting system· and shall ensure that information provided to them is understandable.

O.OSP.Availability [un] [non-core] The ·remote electronic voting system· should be available during the whole ·polling phase·.
Appl. Note: The ·remote electronic voting system· shall be robust against power outage at the ·voting server·, unexpected ·user· activity, environmental effects (for instance, mechanical, electromagnetic, and climatic) to the ·voting server·, and network problems.

O.OSP.VoteRightExc [un] [di] The ·remote electronic voting system· shall ensure that in case of exceptions, malfunctions, and breakdowns no ·voter· looses his right to ·cast· a ·vote· nor get the possibility to ·cast· two ·votes·.
Appl. Note: The ·remote electronic voting system· shall be capable to determine whether a particular ·voter· ·cast· a vote and his ·e-vote· was successfully stored in case of exceptions, malfunctions, and breakdowns.

O.OSP.DataLoss [di] The ·remote electronic voting system· shall prevent data loss during normal operations and in case of exceptions, malfunctions, and breakdowns.

O.OSP.ErrorRecovery [di] [un] The ·voting server· shall run a self-check before a resuming is possible. In case of irreversible problems the ·voting server· shall prevent a resuming of the ·polling phase·.

Op.1 [tr] The ·responsible election authority· shall develop a contingency plan describing appropriate responses to at least the following circumstances:

- results produced by recount or alternative ·tallying software· do not agree with original result
- number of ·votes· recorded does not match number of ·electors·
- any kind of exceptions, malfunctions, and breakdowns

O.T.SecretAuthNet [un] The ·remote electronic voting system· shall protect the confidentiality of the transmitted ·authentication information·.

O.T.IntResultNet [fr] The ·remote electronic voting system· shall ensure the confidentiality of the transmitted ·e-votes· during the ·polling phase·.

O.OSP.Transmission [un] The ·client-side voting software· shall immediately transmit the ·e-votes· to the ·voting server·, whenever a ·voter· has ·cast· his ·vote·.

O.T.AC [all] The ·voting server· shall implement an access control policy for the ·poll worker interface· which

- restricts all activities to particular ·user·-roles and
- requires physical presence.

O.OSP.SepDuty [all] The access control mechanism shall only allow access to the ·voting server· if at least two different ·users· are logged on.

O.T.IneligVoter [eq] The ·remote electronic voting system· shall unambiguously identify and authenticate the ·voter· before storing his ·vote· in the ·e-ballot box·.

Op.7 [all] The ·responsible election authority· shall develop procedures covering all stages of the ·election·, including

- secure ·voting server· storage at all times
- ·voting server· configuration (including ·ballot· details, order on ·voting server·, and ·tallying software·)
- checking ·voting server· (including configuration and empty ·e-ballot box·)
- response to any kind of exceptions, malfunctions, and breakdowns
- recording of ·poll worker· activities, ·voting server· state changes, system resuming, etc.
- ensuring that the ·voting server· is in the appropriate state at every stage in the ·election phase·.

- closing the ·poll(s)·, including disabling ·voting server·
- tallying and re-tallying
- comparing number of ·votes· recorded with number of ·electors·
- ·archiving phase·, including data deletion at the end
- ·identification and authentication token· delivery, their storage and management where necessary

O.T.WrongSW [all] The ·voting server· shall communicate only with the authentic and unaltered ·client-side voting software·.

O.T.WrongServer [all] The ·client-side voting software· shall only communicate with the authentic and unaltered ·voting server·.

O.T.DeleteMsgNet [un] [tr] The ·remote electronic voting system· shall ensure that protocol messages cannot be deleted undetected.

O.T.AlterMsgNet [all] The ·remote electronic voting system· shall verify the freshness, authenticity, integrity, and format correctness of all messages before processing them.

O.T.TamperServer [all] The ·voting server· should be tamper-resistant. The ·voting server· shall be tamper-evident.

O.T.TamperClient [all] The ·client-side voting software· shall ensure that its operations and data are unaffected by other applications running on the ·vote-casting device·.

O.T.IntegVotes [di] The ·voting server· shall protect the integrity and authenticity of ·e-votes· after the ·polling phase·.

O.T.IntegElecData [di] The ·tallying software· shall protect the integrity and authenticity of ·election data· as soon as the tallying is completed.

O.OSP.PWInterface [se] [fr] The only functionality provided by the ·poll worker interface· is

- identification and authentication,
- starting the ·polling phase· which is only possible once,
- resuming the ·polling phase· after any kind of exceptions, malfunctions, and breakdowns according to O.OSP.ErrorRecovery,
- closing the ·polling phase· after which the actions 'starting' and 'resuming' are disabled,
- starting the ·tallying phase· only after having closed the ·polling phase·,
- performing self-checks,

- checking that the ·voting server· has been set up correctly (for example, order of ·voting options· and empty ·e-ballot box·),
- checking the current state according to O.OSP.InfoPW, and
- reading the audit trails.

Appl. Note: The ·voting server· shall not provide any functionality to reach any of the intruder's goals described in section 4.3. (A/N: This refers to [109].)

O.OSP.SelfCheck [all] The ·voting server· should regularly perform automatic self-checks and report the results to the ·poll workers·. The ·voting server· shall be capable of performing self-checks.

O.OSP.DeleteData [di] The ·voting server· shall provide the functionality to completely delete all data from previous ·elections·.

O.OSP.ClosePoll [un] [non-core] The acceptance of ·e-votes· into the ·e-ballot box· should remain open for a sufficient phase of time to allow for any delay of data transport.

O.OSP.PWClosePoll [un] The ·poll worker interface· shall warn the ·poll workers· if they try to close the ·election· before the final date.

O.OSP.AccurDisp [fr] The ·voting server· shall accurately display the authentic and unaltered ·ballot·.

O.OSP.EqualPres [fr] The ·client-side voting software· shall ensure equality and accuracy of presentation of ·voting options· on any ·vote-casting device·.
Appl. Note: The ·remote electronic voting system· shall avoid the display of other influencing messages.

Op.13 [fr] [non-core] The ·responsible election authority· should ensure that all ·electronic voting system· display the ·ballot· in a uniform way.

O.OSP.Interface [fr] The ·client-side voting software· shall provide the following functionality for the ·voter·:

- Identification and authentication
- Make a choice on the ·ballot·
- Change ·selections· before ·casting a vote·
- Initialise vote casting
- ·Vote casting·
- Cancel his ·voting process· at any time

O.OSP.Spoil [fr] [non-core] The ·client-side voting software· should provide the functionality for the ·voter· to ·spoil· his ·vote·.

O.OSP.SpoilWarning [fr] [non-core] The ·client-side voting software· should warn the ·voter· when he tries to ·spoil· his ·vote· in one or more ·polls·.

O.OSP.Confirmation [tr] The ·remote electronic voting system· shall provide a confirmation to the ·voter· regarding the status of his ·vote· – at least the information that his ·e-vote· has been successfully stored.
Appl. Note: In case the ·voter· does not receive the confirmation, he shall get this information as soon as he logs on again.

O.T.ProofGen [se] The remote electronic voting system shall ensure that voters are not able to construct a receipt proving their vote. Neither information sent to, displayed on, sent from, nor intermediate results calculated on his vote-casting device or protocol messages sequences shall serve as proof.

O.T.ElecSecrecyNet [fr] The ·remote electronic voting system· shall not provide any information in the transmitted protocol messages, which allows to construct the link between a particular ·voter· and his ·vote·. The ·remote electronic voting system· shall ensure that neither the ·vote· itself nor the number of chosen ·voting options· (including an empty ·ballot·), nor a ·spoilt· ·vote· (for example, by using the length of the protocol messages) can be linked to a particular ·voter·. In addition, it shall be ensured that the sequence of messages does not reveal the link.

Op.5 [un] The ·responsible election authority· shall coordinate the different channels, for instance, it shall prevent ·voters· ·casting one vote· per possible channel and shall develop a procedure to merge the results from different channels.

O.T.AuthCheckCount [di] The ·tallying software· shall verify the integrity and authenticity of ·e-votes·.

O.T.AffectCounting [di] The ·tallying software· shall ensure that its operations and data are unaffected by other applications.

O.OSP.AccurCalc [di] The ·tallying software· shall accurately calculate results using the appropriate algorithm based on all (authorised) ·e-votes· stored in the ·e-ballot box· and only based on these ·e-votes·.

Op.11 [tr] [non-core] The ·responsible election authority· should arrange alternative ·tallying software· to check results.

O.OSP.ReadToOtherSystems [tr] The ·remote electronic voting system· shall provide the functionality to upload ·e-votes· into any ·tallying software·.

O.OSP.Auditing [tr] The ·voting server· shall be capable of producing comprehensive audit data.

O.OSP.Audit1 [tr] The ·audit system· shall provide the functionality to record, monitor, and verify audit data.

O.OSP.Audit2 [tr] The ·audit system· shall protect the integrity and authenticity of audit records.

O.OSP.Audit3 [tr] The ·audit system· shall have access to a reliable time source.

O.OSP.Audit4 [tr] The ·audit system· shall record system configuration (including software version numbers) and·election· configuration (including ·voting option· information) on the ·voting server· at least at the following points

- beginning and end of ·polling phase·, as well as
- before and after tallying.

O.OSP.Audit5 [tr] The ·audit system· shall check the ·e-ballot box·, the ·ballot· content, and the ·authentication data· for evidence of tampering.

O.OSP.Audit6 [tr] The ·audit system· and its records should be tamper-resistant and shall be tamper-evident.

O.OSP.Audit7 [tr] For every action performed by ·poll workers· the ·audit system· shall record

- a timestamp,
- the nature of the action, and
- the ID of the particular ·poll worker·(where available).

O.OSP.Audit8 [tr] The ·audit system· shall record (with timestamps, where appropriate)

- breakdowns,
- exceptions,
- malfunctions, and
- results of any self-checks.

O.OSP.Audit9 [tr] The ·audit system· shall implement the access control policy defined by the ·responsible election authority·.

O.OSP.Audit10 [tr] The ·audit system· should not record any information which might endanger the secrecy of the vote. Where such information is stored it shall only be accessible to those with appropriate authority.

O.T.ElectionSecrecy [se] The voting server should not store any information which could link the voter with his vote after the completion of the voting process. Where any information which could link the voter to his vote is stored on the voting server, it shall only be accessible to those with appropriate authority.

O.OSP.SecrecyAfterBreakd [se] In case of exceptions, malfunctions, and breakdowns, the voting server shall not reveal the link from the last voter to his selections or vote.

O.T.DeleteRecord [se] The remote electronic voting system shall delete any records related to the voter's voting process from the vote-casting device when finishing the voting process.

Op.9 [fr] [un] The ·responsible election authority· shall educate ·voters· in the use of the ·electronic voting system· and shall ensure that the information provided to them is understandable.

O.T.PersonalDataNet [dp] The ·remote electronic voting system· shall ensure the data protection law with respect to the transmission of any personal data.

O.OSP.Audit11 [dp] The ·audit system· shall ensure the data protection law.

Bibliography

[1] European Privacy Seal – EuroPriSe Criteria. https://www.european-privacy-seal.eu/criteria/EuroPriSe%20Criteria%20Catalogue%20public%20version%201.0.pdf. Version 1.0.

[2] EuroPriSe – European Privacy Seal. https://www.european-privacy-seal.eu/.

[3] Federal Constitution for the Federal Republic of Germany (Grundgesetz für die Bundesrepublik Deutschland). http://www.bundestag.de/dokumente/rechtsgrundlagen/grundgesetz/gg.html (english translation: https://www.btg-bestellservice.de/pdf/80201000.pdf).

[4] German Civil Code (Bürgerliches Gesetzbuch). http://www.gesetze-im-internet.de/englisch_bgb/index.html.

[5] German Federal Central Criminal Register Act (Bundeszentralregistergesetz). http://www.gesetze-im-internet.de/bzrg/index.html.

[6] German Federal Data Protection Act (Bundesdatenschutzgesetz). http://www.gesetze-im-internet.de/bdsg_1990/.

[7] German Federal Electoral Act (Bundeswahlgesetz). http://www.gesetze-im-internet.de/bwahlg/index.html.

[8] German Federal Network Agency (Bundesnetzagentur). http://www.bundesnetzagentur.de/.

[9] German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI). http://www.bsi.de/.

[10] German Teleservices Act (Telemediengesetz). http://www.gesetze-im-internet.de/tmg/.

[11] German Works Constitution Act (Betriebsverfassungsgesetz). http://www.gesetze-im-internet.de/betrvg/.

[12] Gesetz über Ordnungswidrigkeiten (engl. German Administrative Offences Act). http://www.gesetze-im-internet.de/owig_1968/index.html.

[13] Independent Centre for Privacy Protection Schleswig-Holstein (ICPP) (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein). https://www.datenschutzzentrum.de/faq/guetesiegel_engl.htm.

[14] IT-Grundschutz Catalogues – B 1.5 Data Privacy Protection. https://www.bsi.bund.de/cae/servlet/contentblob/475580/publicationFile/31384/moduleb01005_pdf.pdf.

[15] Tüvit. http://www.tuvit.de/english/Overview.asp.

[16] German Federal Electoral Ordinance (Bundeswahlordnung). http://www.gesetze-im-internet.de/bundesrecht/bwo_1985/gesamt.pdf, 1985.

[17] Austrian Students Association Act (in german: Hochschülerinnen- und Hochschülerschaftsgesetz, HSG). http://www.bmwf.gv.at/wissenschaft/national/gesetze/studienrecht/hsg_1998/, 1998.

[18] German Federal Voting Machines Ordinance (Bundeswahlgeräteverordnung). http://www.gesetze-im-internet.de/bwahlgv/index.html, 1999.

[19] German Ordinance for Implementing the Works Constitution Act (Erste Verordnung zur Durchführung des Betriebsverfassungsgesetzes (Wahlordnung – WO)). http://www.gesetze-im-internet.de/bundesrecht/betrvgdv1wo/gesamt.pdf, 2001.

[20] Austrian Students Association Ordinance (in german: Hochschülerinnen- und Hochschülerschaftswahlordnung, HSWO). http://www.bmwf.gv.at/wissenschaft/national/gesetze/studienrecht/hswo_2005/, 2005.

[21] Republic and Canton of Geneva State Chancellery: Report by the Geneva government to the Geneva parliament on the Internet voting project. http://www.ge.ch/evoting/english/doc/rapports/EN_RD_639_and_Annex.pdf, 2007.

[22] ISO/IEC 27001:2005 Information Technology – Security Techniques – Information Security Management Systems Requirements Specification, 2008.

[23] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model. http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R3.pdf, July 2009. Version 3.1 Revision 3 Final.

[24] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components. http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R3.pdf, July 2009. Version 3.1 Revision 3 Final.

[25] Common Methodology for Information Technology Security Evaluation – Evaluation methodology. http://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R3.pdf, July 2009. Version 3.1 Revision 3 Final.

[26] Yearly Report on Algorithms and Keysizes. http://www.ecrypt.eu.org/documents/D.SPA.13.pdf, March 2010. D.SPA.13 Revision 1.0, ICT-2007-216676, ECRYPT II.

[27] Ben Adida. Helios: web-based open-audit voting. In *SS'08: Proceedings of the 17th conference on Security symposium*, pages 335–348, Berkeley, CA, USA, 2008. USENIX Association.

[28] Ben Adida, Olivier de Marneffe, Olivier Pereira, and Jean-Jacques Quisquater. Electing a University President Using Open-Audit Voting: Analysis of Real-World Use of Helios. In T. Moran D. Jefferson, J.L. Hall, editor, *Electronic Voting Technology Workshop / Workshop on Trustworthy Elections (EVT/WOTE)*. Usenix, 8 2009.

[29] Riza Aditya, Colin Boyd, Ed Dawson, and Kapali Viswanathan. Secure e-voting for preferential elections. In Roland Traunmüller, editor, *EGOV*, volume 2739 of *Lecture Notes in Computer Science*, pages 246–249. Springer, 2003.

[30] Riza Aditya, Byoungcheon Lee, Colin Boyd, and Edward Dawson. Implementation Issues in Secure E-Voting Schemes. In E Kozan, editor, *Proceedings of Abstracts and Papers (On CD-Rom) of the Fifth Asia-Pacific Industrial Engineering and Management Systems (APIEMS) Conference 2004 and the Seventh Asia-Pacific Division Meeting of the International Foundation of Production Research*, pages 1–14, Gold Coast, Australia, 2004. Queensland University of Technology.

[31] Austrian Federal Ministry of Science and Research. E-Voting bei den Hochschülerinnen- und Hochschülerschaftswahlen 2009 – Evaluierungsbericht. `http://www.e-voting.cc/stories/6271873/`, 2010.

[32] Elaine Barker, William Barker, William Burr, William Polk, and Miles Smid. Recommendation for key management - part 1: General (revised). In *NIST Special Publication*, number 800-57, 2007.

[33] Jordi Barrat. The certification of e-voting mechanisms – Discussion paper. `http://www.coe.int/t/dgap/democracy/Activities/GGIS/E-voting/E-voting_2009/Workshop_Nov2009/Discussion_paper_E_pdf.pdf`. Council of Europe (November 9/10th 2009).

[34] Olivier Baudron, Pierre-Alain Fouque, David Pointcheval, Jacques Stern, and Guillaume Poupard. Practical Multi-Candidate Election System. In *PODC'01: Proceedings of the twentieth annual ACM symposium on Principles of distributed computing*, pages 274–283, New York, NY, USA, 2001. ACM.

[35] BlueKrypt. Cryptographic Key Length Recommendations. `http://www.keylength.com/`, 2010.

[36] S. Bradner. Key words for use in RFCs to Indicate Requirement Levels. RFC 2119 (Best Current Practice), March 1997.

[37] Nadja Braun and Daniel Brändli. Swiss E-Voting Pilot Projects: Evaluation, Situation Analysis and How to Proceed. In Robert Krimmer, editor, *Electronic Voting*, volume 86 of *Lecture Notes in Informatics*, pages 27–36. GI, 2006.

[38] Johannes Buchmann and Alexander Roßnagel. Das Bundesverfassungsgericht und Telemedienwahlen. *Kommunikation und Recht*, Heft 9:543, 2009.

[39] Österreichische HochschülerInnenschaft Bundesvertretung. About the ÖH. `http://www.oeh.ac.at/en/about_oeh/`.

[40] Österreichische HochschülerInnenschaft Bundesvertretung. ÖH-Wahl 2009. `http://www.oeh.ac.at/ueber_die_oeh/oeh_wahlen/wahl_09/`.

[41] Mike Burmester and Emmanouil Magkos. Towards Secure and Practical E-Elections in the New Era. In Dimitris Gritzalis, editor, *Secure Electronic Voting*, volume 7 of *Advances in Information Security*, pages 63–76. Kluwer Academic Publishers, 2003.

[42] The official website of the Common Criteria Project. `http://www.commoncriteriaportal.org/`.

[43] Austrian Federal Computing Centre. `http://www.brz.gv.at`.

[44] David Chaum, Richard Carback, Jeremy Clark, Aleksander Essex, Stefan Popoveniuc, Ronald L. Rivest, Peter Y. A. Ryan, Emily Shen, and Alan T. Sherman. Scantegrity II: End-to-End Verifiability for Optical Scan Election Systems using Invisible Ink Confirmation Codes. In *Proceedings of the conference on Electronic Voting Technology*, EVT'08, pages 14:1–14:13, Berkeley, CA, USA, 2008. USENIX Association.

[45] David Chaum, Peter Ryan, and Steve Schneider. A Practical Voter-Verifiable Election Scheme. In Sabrina di Vimercati, Paul Syverson, and Dieter Gollmann, editors, *Computer Security - ESORICS 2005*, volume 3679 of *Lecture Notes in Computer Science*, pages 118–139. Springer, 2005.

[46] David L. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24(2):84–90, 1981.

[47] George F. Coulouris, Jean. Dollimore, and Tim Kindberg. *Distributed Systems: Concepts and Design*. Addison-Wesley, Wokingham, Sydney, 1994.

[48] Council of Europe. *Legal, Operational and Technical Standards for E-voting*. Council of Europe Publishing, Strasbourg, recommendation rec(2004)11 edition, 2004.

[49] Ronald Cramer, Rosario Gennaro, and Berry Schoenmakers. A Secure and Optimally Efficient Multi-Authority Election Scheme. In *EUROCRYPT*, pages 103–118, 1997.

[50] datenschutz nord GmbH. Kurzgutachten zur Zertifizierung des Produkts Digitales Wahlstiftsystem dotVote (Version 1.0). `https://www.datenschutzzentrum.de/guetesiegel/kurzgutachten/g081007/g081007-kurzgutachten-digitales-wahlstiftsystem-dotVote.pdf`, September 2008.

[51] Jordi Barrat Esteve. The Certification of E-Voting Mechanisms. Fighting against Opacity. In Krimmer and Grimm [83], pages 197–206.

[52] European Parliament and Council of the European Union. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal*, L 281:31–50, 1995.

[53] European Parliament and Council of the European Union. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). *Official Journal*, L 201:37–47, 2002.

[54] German Federal Office for Information Security. Zertifizierte IT-Sicherheit – Prüfstandards für IT-Sicherheit, Technische Richtlinien und Schutzprofile, Konformitätsbewertung, Zertifizierung und Anerkennung. `https://www.bsi.bund.de/cae/servlet/contentblob/476492/publicationFile/51093/zertifizierte-IT_pdf.pdf`.

[55] Organization for Security, Office for Democratic Institutions Co-operation in Europe (OSCE), and Human Rights (ODIHR). *OSCE/ODIHR Election Assessment Mission Report on the 2007 parliamentary elections in Estonia*, 2007. `http://www.osce.org/item/25385.html`.

[56] French Network and Information Security Agency (FNISA). Mécanismes cryptographiques - Règles et recommandations. `http://www.ssi.gouv.fr/IMG/pdf/RGS_B_1.pdf`, 2010. Revision 1.20.

[57] German Federal Constitutional Court (Bundesverfassungsgericht). Judgment of 3 march 2009, 2 bvc 3/07 and 2 bvc 4/07. `http://www.bundesverfassungsgericht.de/entscheidungen/cs20090303_2bvc000307.html`.

[58] German Federal Constitutional Court (Bundesverfassungsgericht). Use of voting computers in 2005 Bundestag election unconstitutional. `http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg09-019en.html`. Press release no. 19/2009 of 3 March 2009.

[59] German Federal Office for Information Security. *IT-Grundschutz Catalogues*, 2005. `https://www.bsi.bund.de/cln_174/EN/topics/ITGrundschutz/ITGrundschutzCatalogues/itgrundschutzcatalogues_node.html`.

[60] German Federal Office for Information Security. Biometric Verification Mechanisms Protection Profile. `https://www.bsi.bund.de/cae/servlet/contentblob/480264/publicationFile/29296/pp0043b_pdf.pdf`, 2008.

[61] German Federal Office for Information Security. *BSI-Standard 100-1 Information Security Management Systems (ISMS)*, 1.5 edition, 2008.

[62] German Federal Office for Information Security. *BSI-Standard 100-2 IT-Grundschutz Methodology*, 2.0 edition, 2008.

[63] German Federal Office for Information Security. *BSI-Standard 100-3 Risk analysis based on IT-Grundschutz*, 2.5 edition, 2008.

[64] German Federal Office for Information Security. Common Criteria Protection Profile for Basic set of security requirements for Online Voting Products. `https://www.bsi.bund.de/cae/servlet/contentblob/480286/publicationFile/29585/pp0037b_engl_pdf.pdf`, 2008. BSI-CC-PP-0037.

[65] German Federal Office for Information Security. *IT-Grundschutz-Kataloge*, Stand 10. Ergänzungslieferung edition, 2008. `https://www.bsi.bund.de/cln_174/ContentBSI/grundschutz/kataloge/kataloge.html`.

[66] German Federal Office for Information Security. Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz - Prüfschema für ISO 27001-Audits, 2008.

[67] German Federal Office for Information Security. Zertifizierungsreport BSI-CC-PP-0037-2008. `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ReportePP/pp0037a_pdf.pdf?__blob=publicationFile`, 2008.

[68] German Federal Office for Information Security. Common Criteria Protection Profile Electronic Identity Card (ID_Card PP). `https://www.bsi.bund.de/cae/servlet/contentblob/850458/publicationFile/51724/pp0061b_pdf.pdf`, 2009. BSI-CC-PP-0061.

[69] German Federal Office for Information Security. Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen). `http://www.bundesnetzagentur.de/cln_1912/DE/Sachgebiete/QES/Veroeffentlichungen/Algorithmen/algorithmen_node.html`, 2011.

[70] Gesellschaft für Informatik. Wahlen und Ordnungen. `http://www.gi-ev.de/wir-ueber-uns/leitung/wahlen-und-ordnungen/`.

[71] Object Management Group. Unified Modeling Language. `http://www.uml.org/`.

[72] Volker Hammer, Ulrich Pordesch, and Alexander Roßnagel. KORA – eine Methode zur Konkretisierung rechtlicher Anforderungen zu technischen Gestaltungsvorschlägen für Informations- und Kommunikationssysteme. Technical Report Arbeitspapier 100, provet, Darmstadt, 1992.

[73] Volker Hammer, Ulrich Pordesch, and Alexander Roßnagel. Betriebliche Telefon- und ISDN-Anlagen rechtsgemäß gestaltet. Berlin, 1993.

[74] Volker Hammer, Ulrich Pordesch, Alexander Roßnagel, and Michael J. Schneider. Vorlaufende Gestaltung von Telekooperationstechnik am Beispiel von Verzeichnisdiensten, Personal Digital Assistants und Erreichbarkeitsmanagement in der Dienstleistungsgesellschaft. GMD Studie Nr. 235, 1994. Gesellschaft für Mathematik und Datenverarbeitung mbH.

[75] Volker Hartmann, Nils Meissner, and Dieter Richter. Online Voting Systems for Non-parliamentary Elections – Catalog of Requirements. Laborbericht PTB-8.5-2004-1, Physikalisch-Technische Bundesanstalt Braunscheig und Berlin (Fachbereich Metrologische Informationstechnik), May 2004. `http://ib.ptb.de/8/85/LB8_5_2004_1AnfKat.pdf`.

[76] Martin Hirt and Kazue Sako. Efficient Receipt-Free Voting Based on Homomorphic Encryption. In Bart Preneel, editor, *EUROCRYPT*, volume 1807 of *Lecture Notes in Computer Science*, pages 539–556. Springer, 2000.

[77] Sabrina Idecke-Lux. *Der Einsatz von multimedialen Dokumenten bei der Genehmigung von neuen Anlagen nach dem Bundesimmissionsschutz-Gesetz*. Nomos, 2000. Baden-Baden.

[78] Rui Joaquim, Andre Zuquete, and Paulo Ferreira. REVS – A Robust Electronic Voting System. In *Proceedings of IADIS International Conference e-Society 2003*, pages 95–103, 2003.

[79] Ari Juels, Dario Catalano, and Markus Jakobsson. Coercion-Resistant Electronic Elections. In Vijay Atluri, Sabrina De Capitani di Vimercati, and Roger Dingledine, editors, *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, pages 61–70. ACM, 2005.

[80] Heinrich Kersten, Jürgen Reuter, and Klaus-Werner Schröder. *IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz*. Vieweg, 2008.

[81] Steve Kremer, Mark Ryan, and Ben Smyth. Election verifiability in electronic voting protocols. In *Proceedings of the 15th European conference on Research in computer security*, ESORICS'10, pages 389–404, Berlin, Heidelberg, 2010. Springer.

[82] Robert Krimmer, Andreas Ehringfeld, and Markus Traxl. The Use of E-Voting in the Austrian Federation of Students Elections 2009. In Robert Krimmer and Rüdiger Grimm, editors, *Electronic Voting*, volume 167 of *Lecture Notes in Informatics*, pages 33–44. GI, 2010.

[83] Robert Krimmer and Rüdiger Grimm, editors. *3rd International Conference, Co-organized by Council of Europe, Gesellschaft für Informatik and E-Voting.CC, August 6th-9th, 2008 in Castle Hofen, Bregenz, Austria*, volume 131 of *Lecture Notes in Informatics*. GI, 2008.

[84] Philip Laue. *Vorgangsbearbeitungssysteme in der öffentlichen Verwaltung*. kassel university press, 2009. PhD thesis.

[85] Byoungcheon Lee, Colin Boyd, Ed Dawson, Kwangjo Kim, Jeongmo Yang, and Seungjae Yoo. Providing Receipt-freeness in Mixnet-based Voting Protocols. In *In Proc. of Information Security and Cryptology (ICISC 2003)*, volume 2971 of *Lecture Notes in Computer Science*, pages 245–258. Springer, 2003.

[86] Byoungcheon Lee and Kwangjo Kim. Receipt-Free Electronic Voting Scheme with a Tamper-Resistant Randomizer. In Pil Joong Lee and Chae Hoon Lim, editors, *Information Security and Cryptology — ICISC 2002, 5th International Conference Seoul, Korea, November 28-29, 2002, Revised Papers*, volume 2587 of *Lecture Notes in Computer Science*, pages 389–406. Springer, 2003.

[87] Emmanouil Magkos, Panayiotis Kotzanikolaou, and Christos Douligeris. Towards Secure Online Elections: Models, Primitives and Open Issues. *Electronic Government*, 4(3):249–268, 2007.

[88] Micromata. Polyas Online Voting Solutions. Online-Wahlen für Verbände und Vereine, 2005. `http://www.micromata.de/produkte/documents/polyas_broschuere_72dpi.pdf`.

[89] D. Mills. Network Time Protocol (Version 3) Specification, Implementation and Analysis. RFC 1305 (Draft Standard), 1992.

[90] C. Andrew Neff. Practical High Certainty Intent Verification for Encrypted Votes. `http://www.votehere.com/old/vhti/documentation/vsv-2.0.3638.pdf`, 2004.

[91] Miyako Ohkubo, Fumiaki Miura, Masayuki Abe, Atsushi Fujioka, and Tatsuaki Okamoto. An Improvement on a Practical Secret Voting Scheme. In Masahiro Mambo and Yuliang Zheng, editors, *Proceedings of the Second International Workshop on Information Security*, volume 1729 of *Lecture Notes in Computer Science*, pages 225–234. Springer, 1999.

[92] provet (Projektgruppe verfassungsverträgliche Technikgestaltung). Entwurf eines Gesetzes zur Regelung von Telemedienwahldiensten für nicht parlamentarische Wahlen und zur Änderung weiterer Vorschriften, Entwurf zu einer Verordnung zur Regelung von Wahldiensteanbietern. Working paper, 2010. Universität Kassel, Germany.

[93] Andreu Riera. An Introduction to Electronic Voting Schemes. Technical Report PIRDI 9-98, University of Barcelona, October 1998. `http://pirdi.uab.es/document/pirdi9.ps`.

[94] Peter Y. A. Ryan, David Bismark, James Heather, Steve Schneider, and Zhe Xia. Prêt à voter: a voter-verifiable voting system. *IEEE Transactions on Information Forensics and Security*, 4(4):662–673, 2009.

[95] Peter Y. A. Ryan and Vanessa Teague. Pretty Good Democracy. In *Proceedings of the 17th International Workshop on Security Protocols*, Lecture Notes in Computer Science. Springer, April 2009.

[96] Krishna Sampigethaya and Radha Poovendran. A Framework and Taxonomy for Comparison of Electronic Voting Schemes. *Elsevier Computers & Security*, 25(2):137–153, March 2006.

[97] Fred B. Schneider. Enforceable Security Policies. *ACM Transactions on Information and System Security*, 3(1):30–50, 2000.

[98] Berry Schoenmakers. Voting Schemes. to appear in ALGORITHMS AND THEORY OF COMPUTATION HANDBOOK (Second Edition), Mikhail Atallah and Marina Blanton (Eds.), CRC-Press, 2009. `http://www.win.tue.nl/~berry/papers/ChVotingSchemesJuly2008.pdf`.

[99] Scytl. Pnyx.core: The Key to Enabling Reliable Electronic Elections. A Description of Scytl's Cryptographic e-Voting Security Software, 2005. `http://www.scytl.com/_a_home/PNYXCOREWhitePaper.pdf`.

[100] Scytl. Election Configuration System. `http://www.scytl.com/images/upload/productos/ElectionConfigurationSystem.pdf`, 2010.

[101] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.

[102] German Electronic Signature Act. `http://www.gesetze-im-internet.de/sigg_2001/index.html`, 2001. english translation: `http://www.bundesnetzagentur.de/media/archive/3612.pdf`.

[103] German Electronic Signature Ordinance. `http://www.gesetze-im-internet.de/sigv_2001/index.html`, 2001. english translation: `http://www.bundesnetzagentur.de/media/archive/3613.pdf`.

[104] Warren D. Smith. Cryptography meets voting. `http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.58.9599`, 2005.

[105] Daniel Sokolov. Österreich: Nur 0,9 Prozent Wahlbeteiligung bei E-Voting. heise online, 2009. `http://www.heise.de/newsticker/Oesterreich-Nur-0-9-Prozent-Wahlbeteiligung-bei-E-Voting--/meldung/138303`.

[106] Tobias Stadler. *Mobiles Bezahlen. Die rechtsverträgliche Gestaltung mobiler Bezahlverfahren in Deutschland*. Der elektronische Rechtsverkehr. Nomos, 2006. PhD thesis.

[107] Sandrine Tranchard. The State of Geneva designs a secure Internet voting system. *ISO Focus*, 6:38–39, October 2009.

[108] Alexander Trechsel. Internet Voting in the March 2007 Parliamentary Elections in Estonia. Report for the Council of Europe, July 2007. `http://www.vvk.ee/public/dok/CoE_and_NEC_Report_E-Voting_2007.pdf`.

[109] Melanie Volkamer. *Evaluation of Electronic Voting – Requirements and Evaluation Procedures to Support Responsible Election Authorities*. PhD thesis, Universität Koblenz-Landau, 2008.

[110] Melanie Volkamer and Rüdiger Grimm. Development of a Formal IT Security Model for Remote Electronic Voting Systems. In Krimmer and Grimm [83], pages 185–196.

List of Publications

[P1] Axel Schmidt, Melanie Volkamer, and Johannes Buchmann. An Evaluation and Certification Approach to Enable Voting Service Providers. In Robert Krimmer and Rüdiger Grimm, editors, *Electronic Voting*, volume 167 of *Lecture Notes in Informatics*, pages 135–148. GI, 2010.

[P2] Axel Schmidt, Melanie Volkamer, and Johannes Buchmann. Towards the Evaluation of Online Voting Systems and Environments. In *Proceedings of IRIS 2010 Internationales Rechtsinformatik Symposion*, Austria, 2010. OCG.

[P3] Axel Schmidt, Dennis Heinson, Lucie Langer, Zoi Opitz-Talidou, Philipp Richter, Melanie Volkamer, and Johannes Buchmann. Developing a legal framework for remote electronic voting. In *E-voting and Identity - Second international conference VOTE-ID 2009*, volume 5767 of *Lecture Notes in Computer Science*, pages 92–105, Luxembourg, 2009. Springer.

[P4] Axel Schmidt, Melanie Volkamer, Lucie Langer, and Johannes Buchmann. Specification of a Voting Service Provider. In *First International Workshop on Requirements Engineering for e-Voting Systems (RE-VOTE) 2009*, IEEE Xplore Digital Library, pages 9–18, Atlanta, Georgia, USA, August 2010. IEEE.

[P5] Axel Schmidt, Melanie Volkamer, Lucie Langer, and Johannes Buchmann. Towards the impact of the operational environment on the security of e-voting. In Stefan Fischer, Erik Maehle, and Rüdiger Reischuk, editors, *INFORMATIK 2009 - Im Focus das Leben*, volume P-154 of *Lecture Notes in Informatics*, pages 1814–1826. Bonner Köllen Verlag, 2009.

[P6] Lucie Langer, Axel Schmidt, and Melanie Volkamer. Verifizierbarkeit elektronischer Wahlen. *eGovernment Review*, 2(4):20–22, July 2009.

[P7] Lucie Langer, Axel Schmidt, and Johannes Buchmann. Ein PKI-basiertes Protokoll für sichere und praktikable Onlinewahlen. In *Proceedings of EDEM 2009 Electronic Democracy Conference*, pages 243–253. OCG, 2009.

[P8] Lucie Langer, Axel Schmidt, and Alex Wiesmaier. From Student Smartcard Applications to the German Electronic Identity Card. In *Proceedings of ECEG 2009*, pages 430–435. ACI, 2009.

[P9] Lucie Langer, Axel Schmidt, and Johannes Buchmann. Secure and Practical Online Elections via Voting Service Provider. In *Proceedings of ICEG 4th International Conference on e-Government 2008*, pages 255–262, UK, 2008. ACI.

[P10] Lucie Langer and Axel Schmidt. Onlinewahlen mit Wahldiensteanbieter – das Verbundprojekt voteremote. In Peter Parycek and Alexander Prosser, editors, *Proceedings of EDEM 2008 Electronic Democracy Conference*, number 239, pages 281–290, Austria, 2008. OCG.

[P11] Lucie Langer, Axel Schmidt, and Roberto Araújo. A pervasively verifiable online voting scheme. In *Informatik 2008 Beherrschbare Systeme – dank Informatik*, number 133 in Lecture Notes in Informatics, pages 457–462, Munich, September 2008. GI.